07/27/2010

RICOH

Print Controller Design Guide for Information Security 06A

Version 1.00

Gestetner	Lanier	Savin	Ricoh
DSm416	LD016	816	MP161
DSm416f	LD016f	816f	MP161f
DSm416pf	LD016spf	816mf	MP161spf
DSm715	LD315	9016	MP1500
DSm716	LD316	9021d	MP1600
DSm721d	LD320d	9016s	MP2000
DSm716s	LD316L	9021ds	MP1600L
DSm721ds	LD320Ld		MP2000L
DSm625	LD125	7025	MP2500
DSm725e	LD325	8025e	MP2510
DSm730e	LD330	8030e	MP3010
DSm735e	LD335	8035e	MP3500
DSm745e	LD345	8045e	MP4500
GWD2004	LW324	2404WD	MPW2400
GWD2006	LW336	2406WD	MPW3600

Copyright © 2010 RICOH Americas Corporation. All rights reserved.

Visit our Knowledgebase at: http://www.ricoh-usa.com/support/knowledgebase.asp

Notice:

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

Copyright © 2010 by Ricoh Company Ltd.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

The content of this document, and the appearance, features and specifications of Ricoh products are subject to change from time to time without notice. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Ricoh does not provide legal, accounting or auditing advice, or represent or warrant that our products or services will ensure that you are in compliance with any law. Customer is responsible for making the final selection of solution and technical architectures, and for ensuring its own compliance with various laws such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

Version history:

Version	Issue Date	Revised item
1.00	Jan. 15, 2008	1st release

TABLE OF CONTENTS

1. Overview 4
2. Internal System Configuration 6
2-1 Hardware Configuration 6
2-2 Software Configuration 8
3. Data Security 11
4. Firmware Update 13
5. Authentication, Access Control 17
6. Administrator Settings 22
7. Data Erase/Overwrite 23
8. Data Protection 25
9. Additional Methods for Increased Security 28
10. Job/Access Logs 29
11. Capture (MFP Models Only) 32
12. Principal Machine Functions 36
13. Printer 40
14. Scanner (MFP Models Only) 47
15. FAX (MFP Models Only) 53
16. NetFile (GWWS) 59
17. Data Security Considerations 67
18. Web Applications 70
19. WebDocBox (MFP models only) 72
20. Optional Features 75
21. CSS (Customer Support System) – MFP Models Only 79
22. Copy Data Security Feature 80
23. Device SDK Applications (DSDK) 83
24. Data Security Considerations 88

1. Overview

This document describes the structural layout and functional operations of the hardware and software for the multi-functional products and laser printers listed below (herein referred to as the “MFP” and “LP”, respectively), which were designed and developed by Ricoh Co. Ltd. (herein referred to as Ricoh), as well as the security of image data and related information handled by MFP/LP internal and peripheral devices.

The explanations will primarily focus on the following, with particular attention to demonstrating how unauthorized access is not possible to local network environments via the CSS and FAX telecommunications lines, nor to any of the data stored in the MFP/LP.

Operational Summaries
Data Flow
Data Security Considerations

Applicable Products

This document applies to the following MFPs/LPs designed and developed by Ricoh:

Product Code	Gestetner	Lanier	Savin	Ricoh
B262 **B292** **B284** **B288**	**DSm416** **DSm416f** **DSm416pf**	**LD016** **LD016f** **LD016spf**	**816** **816f** **816mf**	**MP161** **MP161f** **MP161spf**
B245 **B276** **B277**	**DSm715** **DSm716** **DSm721d** **DSm716s** **DSm721ds**	**LD315** **LD316** **LD320d** **LD316L** **LD320Ld**	**9016** **9021d** **9016s** **9021ds**	**MP1500** **MP1600** **MP2000** **MP1600L** **MP2000L**
D010	**DSm625**	**LD125**	**7025**	**MP2500**
D007 **D008**	**DSm725e** **DSm730e**	**LD325** **LD330**	**8025e** **8030e**	**MP2510** **MP3010**
B291 **B295**	**DSm735e** **DSm745e**	**LD335** **LD345**	**8035e** **8045e**	**MP3500** **MP4500**
B286 **B289**	**GWD2004** **GWD2006**	**LW324** **LW336**	**2404WD** **2406WD**	**MPW2400** **MPW3600**

Note: Some of the hardware (e.g. external I/F) and functions described in this document may not be supported by the end user's machine. For these details, please refer to the Operating Instructions for the specific machine in question.

★ Note:

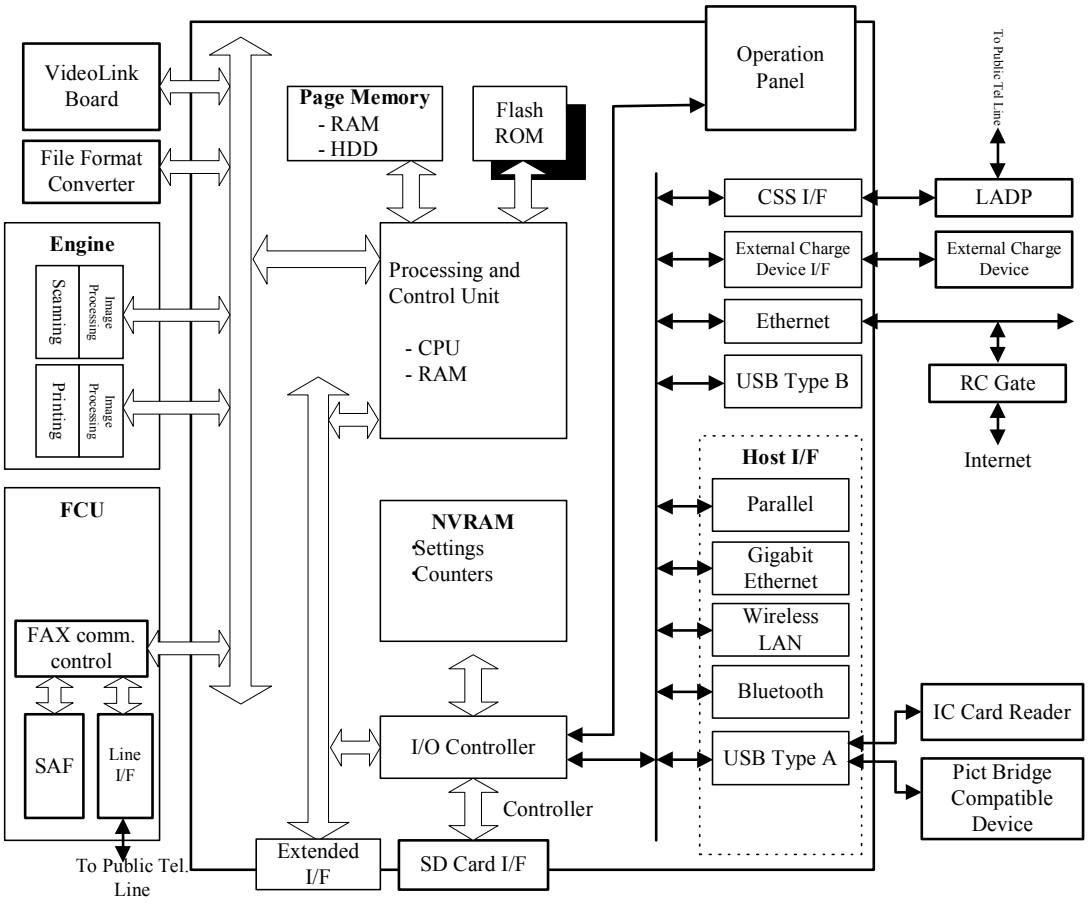
Throughout this document you may see references such as 04A (2004 Autumn) or 05S (2005 Spring). You will only see an A (Autumn) or S (Spring) attached to the last two digits of a year.

These two seasons reflect the time period the machines were manufactured.

2. Internal System Configuration

2-1 Hardware Configuration

MFP



Hardware Configuration

Serial communication between the CSS (Customer Support System) I/F and LADP (Line Adapter).

Serial communication between the external charge device I/F and external coin/card-operated devices.

Image Memory area: Also performs image-processing functions such as data compression and decompression.

Video Link Board: Acts as the interface between the MFP and external controller.

File Format Converter: Converts the file format of image files.

RC Gate: Intermediary device connected to the MFP/LP via an Ethernet connection for performing remote diagnostic operations including firmware updates and settings changes.

SD card I/F: Used for performing service maintenance and as an interface for firmware storage media.

LP

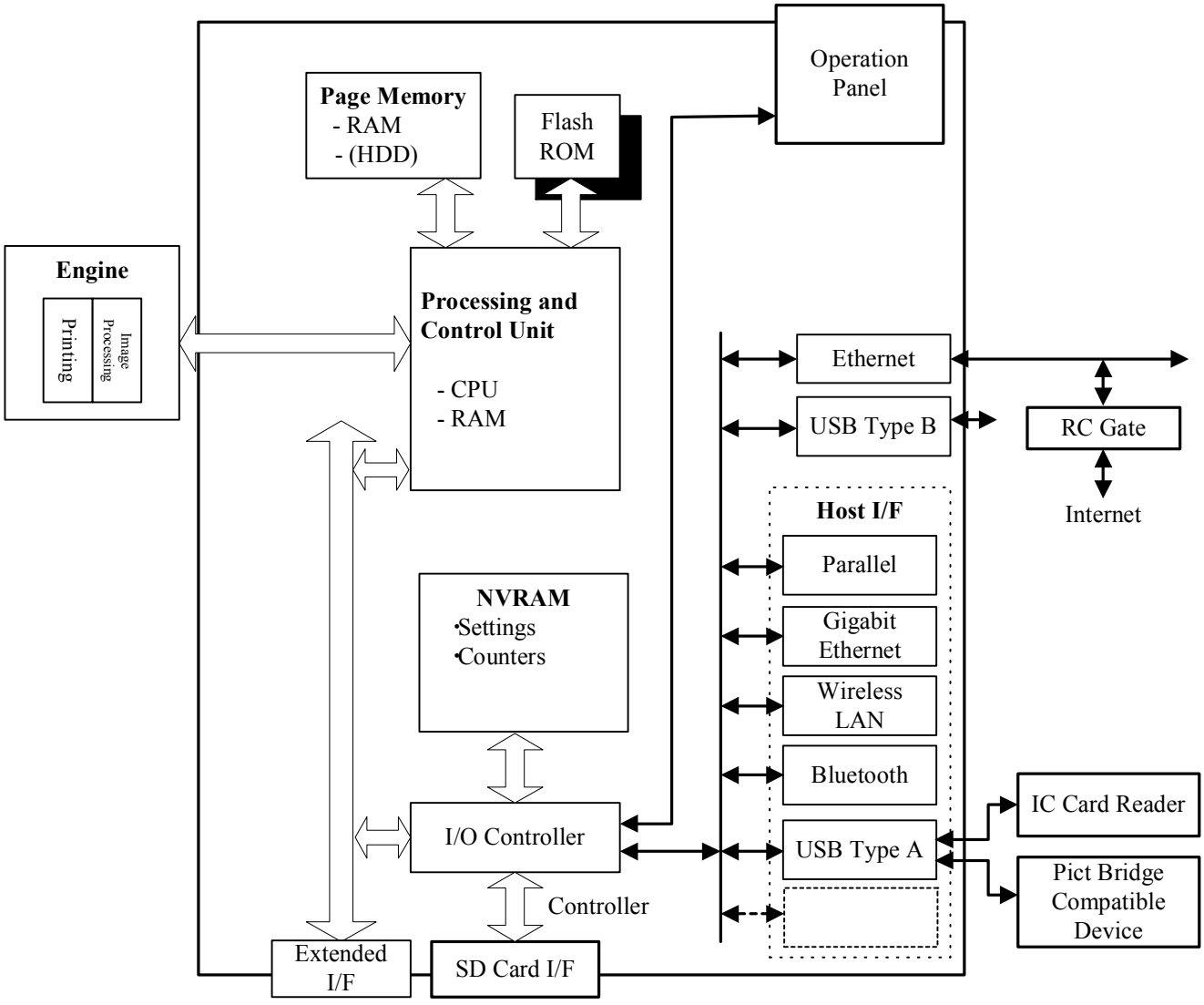
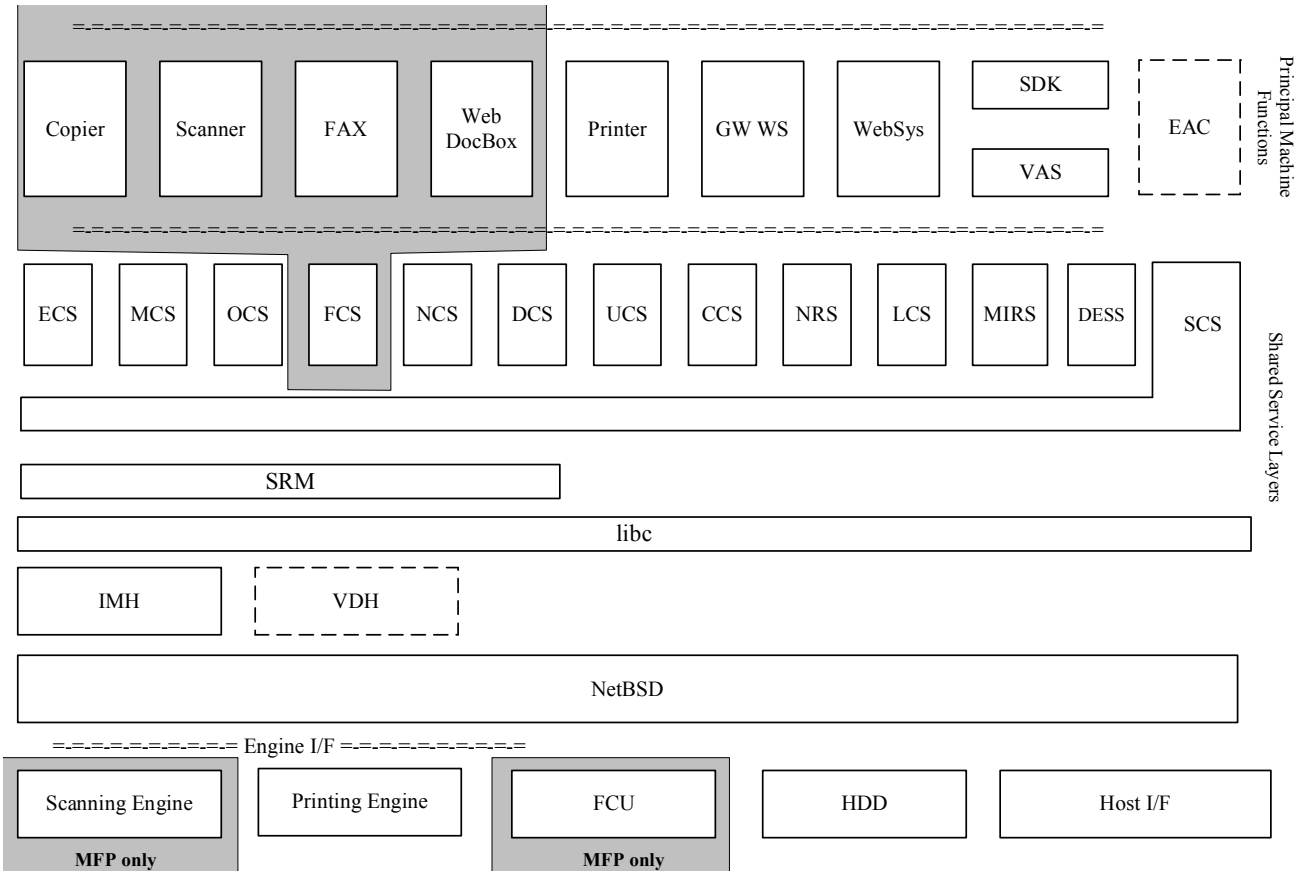


Image Memory area: Also performs image-processing functions such as data compression and decompression.

RC Gate: Intermediary device connected to the LP via an Ethernet connection for performing remote diagnostic operations including firmware updates and settings changes.

SD card I/F: Used for performing service maintenance and as an interface for firmware storage media.

2-2 Software Configuration



Software Configuration

Shared Service Layers

ECS (Engine Control Service)	Controls engine operations for scanning and printing.
MCS (Memory Control Service)	Manages the memory in the Image Memory area (incl. the HDD), as well as compression/decompression.
IMH (Image Memory Handler)	Transfers data between the controller and engine.
OCS (Operation Panel Control Service)	Controls the panel LEDs, monitors panel keys and manages panel objects and display messages.
NCS (Network Control Service)	Controls host I/F and protocol control (transport, session).

FCS (FAX Control Service)	Exchanges data and commands with the FCU (FAX Control Unit), which manages and controls FAX communication and telecommunications lines.
SCS (System Control Service)	Manages the status of all internal operations performed on or by the system as a whole, and controls the switching of the LCD screen as well as the operational link between SP settings and machine operations.
SRM (System Resource Manager)	In addition to managing hardware resources, this module mediates control of the printer engine, scanner engine and memory resources during the image creation process.
DCS (Delivery Control Service)	Controls all non-FAX transmission/reception of email as well ass the forwarding of image data to servers and folders.
MIRS (Machine Information Report Service)	Controls the sending of machine configuration settings by email
UCS (User Control Service)	Manages the Address Book data.
CCS (Certification Control Service)	Mediates communication between the principal machine function and external charge device during the authentication process, as well as the charge-related processing (e.g. counters).
NRS (New Remote Service)	Controls remote correspondence with RC Gate (e.g. diagnostics, firmware update, settings changes).
LCS (Log Control Service)	Controls the MFP/LP's access logs (e.g. Address Book, Document Server, MFP/LP functions).
DESS (Data Encryption Security Service)	Controls the encryption and decryption functions.
VDH (Video Device Handler)	Transfers image data between the MFP engine and external controller. **Note:** This layer exisits only on models capable of supporting an external controller.

Principal Machine Functions

Copier	Activates the scanning engine, which reads the original and then sends the data on to the controller to be printed out from the printing engine. Secondary data, such as that used for access control, is handled from the operation panel.
Printer	Receives image data through the host interface, which then sends the data to the controller. Also contains a printer language processing subsystem (e.g. RPCS) that converts the printer language into image data, which is then printed out from the printing engine. Secondary data is handled via the connection protocols between the driver UI and the host I/F.
Scanner	Activates the scanning engine, which reads the original and then sends the data to a PC via the host I/F. Scanning can be initiated from both the operation panel and from a PC via a TWAIN driver.
FAX	Activates the scanning engine, which reads the original and then sends the data to the FCU to be sent as a FAX via a telecommunications line. Also receives FAX data and prints it out from the printing engine.
Netfile (GWWS)	As a server, GWWS provides some MFP/LP functionality to specific network-connected PC utilities. This includes the ability to view and make changes to user information and machine configuration settings, as well as to print out or perform other operations on documents stored on the MFP/LP. GWWS also acts as a client to external Web services, including transferring the machine log data to specific log data collection utilities
WebSys	Controls Web-based access to the MFP/LP and allows machine configuration settings to be viewed and changed via a Web interface.
WebDocBox	Allows operations to be peformed on Document Server documents stored in the MFP (viewing, downloading, printing, deleting) via a Web interface.
SDK/VAS	SDK: Applications provided by third-party vendors designed to function with MFP/LP pricipal machine functions developed by Ricoh. VAS: An MFP/LP API that standardizes the meanings of simplified commands used by SDK applications when communicating with the MFP/LP.
EAC	The module which controls the serial command flow of the external controller connected via the VideoLink Board, making it possible for the external controller to initiate MFP operations such as print jobs, as well as the storage, deletion, and capturing of Document Server documents. In addition, this module also controls the display content of the MFP LCD for each operation initiated by the controller. **Note:** This is only available on models capable of supporting an external controller.

3. Data Security

External I/F

The MFP/LP is equipped with the following interfaces for connection with external devices:
Serial I/F for LADP connection.
Serial I/F for connection of external coin/card-operated devices.
Serial I/F for connection of peripheral devices (e.g. DF, Finisher, LCT).
Analog G3 FAX I/F (public telecommunications line), G4 FAX I/F (ISDN).
Standard IEEE 1284 parallels I/F (which can function as a two-way parallel interface when using a USB cable).
100BASE-TX and 10BASE-T compatible network I/F
Gigabit Ethernet-compatible network I/F
Standard IEEE802.11b wireless LAN network I/F
Bluetooth I/F
USB2.0 Type B I/F
USB2.0 Type A I/F

Protection of Program Data from Illegal Access via an External Device

1. All of the above principal machine functions, as well as software for all shared service layers, run on the UNIX operating system as independent processes (data/program modules). Memory space is allocated specifically for each module, which makes it impossible for one module to directly access the memory space of any other.
2. Data transfer between modules is Unix socket-based, whereby communication is performed along ID-protected communication paths. This ensures exclusive connections among the modules present in the MFP/LP, thereby preventing access by any module outside this pre-determined set. For example, incoming CSS data will only be sent to those modules designed to perform CSS data operations. This arrangement prevents illegal access to networks and internal programs from an outside line.
3. All image data stored on the HDD or stored temporarily in the Image Memory is managed by a memory control module called the MCS (Memory Control Service), which ensures that the data can only be accessed by specified machine function(s). In addition, this arrangement prevents illegal access to this data from an outside line.

   User data stored in the HDD, such as the Address Book data, is managed by the UCS module. Access to this data is not possible by any module except those pre-determined modules in the MFP/LP itself. This arrangement ensures that the data stored in the MFP/LP cannot be accessed illegally via an external I/F.

4. Communication between the MFP/LP and its peripherals is conducted via the peripheral I/F using Ricoh-unique protocols. These exchanges are limited to pre-determined commands and data, and only take place after the MFP/LP has recognized the peripheral device. If the MFP/LP receives illegal data from the peripheral, it will judge that a perhiperal device failure has occurred or that the device is not connected. This prevents any illegal access to internal programs or data.
5. The MFP communicates with external coin/card-operated devices through the External Charge Device I/F in accordance with the same protocols used for its peripherals described in #4 above. It is possible to utilize such devices in tandem with the access control settings for each user, in which case the device and MFP exchange the relevant information (e.g. User Code data).
6. With the @Remote function, the MFP/LP is connected via the network to a Ricoh-developed device known as RC Gate, which is then connected to the @Remote Center, or to the @Remote Center directly. When connecting to the center directly, the MFP/LP communicates via a LAN connection over the Internet. Before transferring any data, mutual authentication is performed using digital certificates between the MFP/LP and RC Gate or MFP/LP and @Remote Center, which ensures that the MFP/LP cannot connect to any device other than RC Gate or to its single, pre-assigned @Remote Center. Communication between RC Gate/@Remote Center and the MFP/LP modules responsible for @Remote operations is performed over exclusive socket-based connections, as described in #2 above. In addition, it is also possible to change the MFP/LP settings to prohibit @Remote communication.
7. Communication with an external controller is performed via the VideoLink board over a serial connection, which uses a Ricoh-original communication protocol. The internal arrangement is designed such that the external controller cannot gain access to the MFP internal modules until after it has successfully cleared the device registration process.

   In addition, although the external controller is capable of operations such as issuing printing instructions, sending data for storage in the MFP Document Server and downloading/restoring data to and from the MFP, the controller is not able to alter any of the original files already stored in the MFP. (e.g. When the controller restores a file back to the MFP, it is always saved as a separate file).
8. The standard IEEE1284 parallel I/F, USB I/F (Type B), and Bluetooth I/F treat all incoming data as print data. This print data can only be sent to pre-specified modules responsible for executing printing operations. In addition, using MFP/LP settings, it is possible to disable each interface individually.

9. The USB I/F (Type A) only allows connection with devices that support either IC card-based authentication or PictBridge printing functions. Each function can be enabled/disabled individually.

   PictBridge printing functions (color MFP/LPs only):
   After the identity of the connected PictBridge device is verified, the interface and device exchange only pre-defined commands and/or data. Access to data stored inside the MFP/LP is not possible. In addition, if User Authentication has been enabled, the machine will not accept commands or data from any PictBridge functions that do not require authentication.

   IC card-based authentication functions:
   Authentication is mutual and encrypted, which prevents impersonation and ensures that data is properly protected.

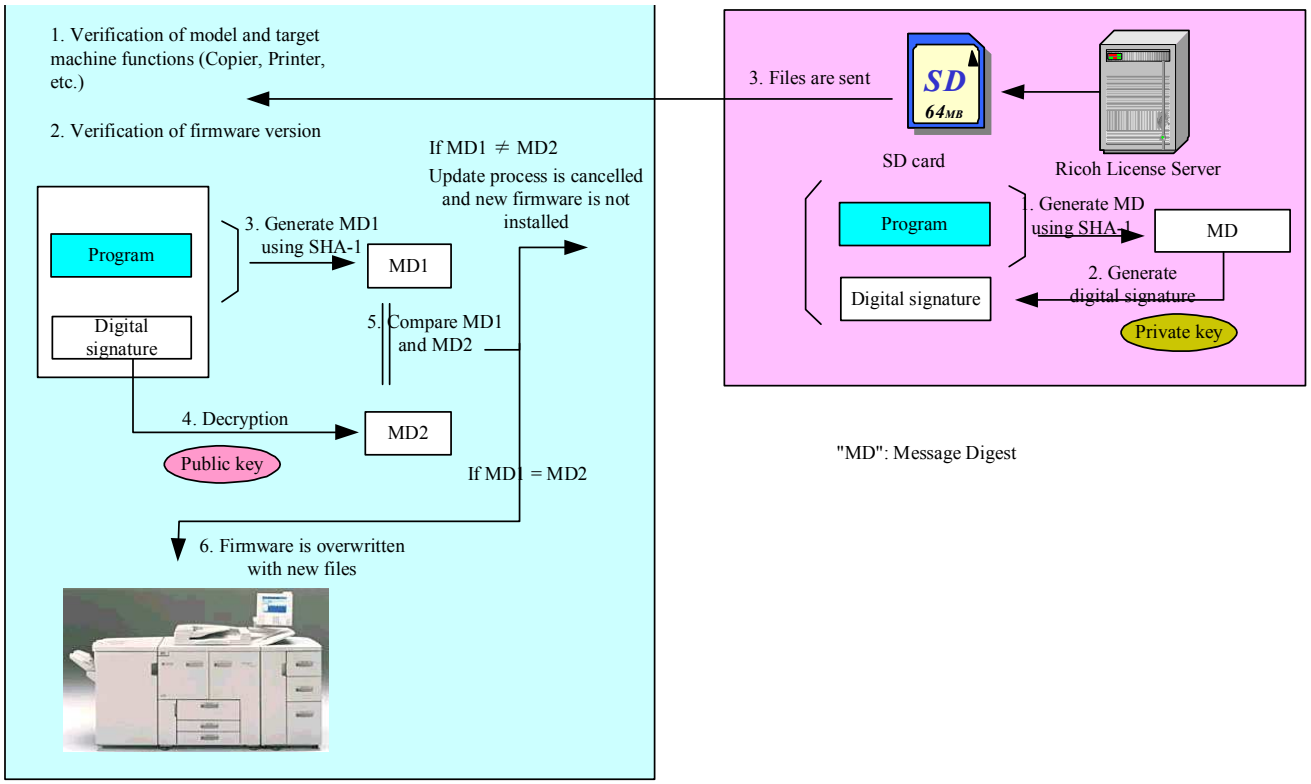
4. Firmware Update

It is possible to update the firmware and application programs stored in the MFP/LP using an SD card or via a remote connection.

Firmware Installation Using an SD Card

- Since SD cards themselves are generic items that are widely available for purchase in the field, the following process is used to prevent the illegal introduction of data and programs into the MFP/LP via this storage media. Briefly stated, a license server assigns a digital signature to the software, which is then used by the MFP/LP to authenticate the program.
  1. The Ricoh license server applies the SHA-1 algorithm (Secure Hash Algorithm 1) to the program to generate the value MD1. A private key is used to encrypt this value, which is then used as the firmware's digital signature.
  2. The firmware in the SD card is introduced into the MFP/LP from the SD card slot.
  3. The MFP/LP checks the firmware to identify the type (e.g. Printer, FAX, Copier), verify that the model name is the same as its own, and verify that the firmware version is newer that the one already installed.
  4. The MFP/LP then applies SHA-1 to the program to generate MD1, after which it uses a public key to decrypt the digital signature to generate MD2.
  5. If MD1 = MD2, the firmware update process begins.

- This use of a public key to decrypt the digital signature allows the MFP/LP to verify that that there has been no illegal alteration of the data.
- The basic identifying information of the firmware (version, type, etc.) is stored in the MFP/LP as the update is being performed. Therefore it is possible to retry the update with the same SD card in the event that the update is interrupted, e.g. if the MFP/LP main power suddenly turns off. After recovery is initiated, the MFP/LP checks to see that the data in the SD card has not been altered, and then resumes the update.



Firmware Installation Using an SD Card

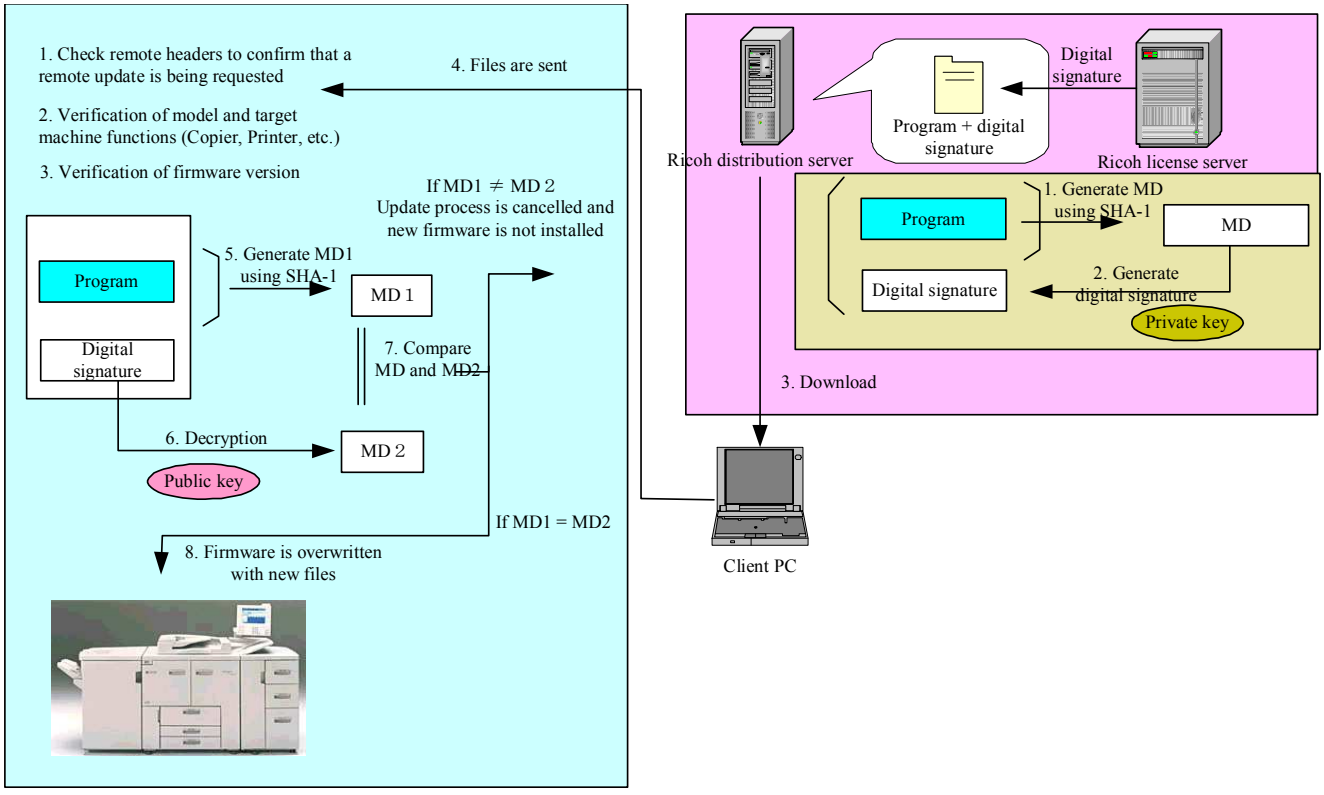
Remote Firmware Installation

- In addition to using an SD card, it is also possible to update the firmware by transmitting the firmware files to the MFP/LP via a remote connection. Since these files are transmitted over public Internet communication paths in some cases, routed through multiple servers before reaching their destination, it is necessary to use the authentication process described above for remote update as well. The process for remote updates is virtually the same as that for the SD card-based update described above, with the following differences:
- Remote headers are attached to the digital signature before sending the files to the MFP/LP. If the update is interrupted for some reason, e.g. a power cut before the update is completed, it is possible to retry the update by resending the file.
- There are three main scenarios in which a remote firmware update is performed, the process for which is the same (see illustrations below). In addition, all of the security features described above are used in each case.

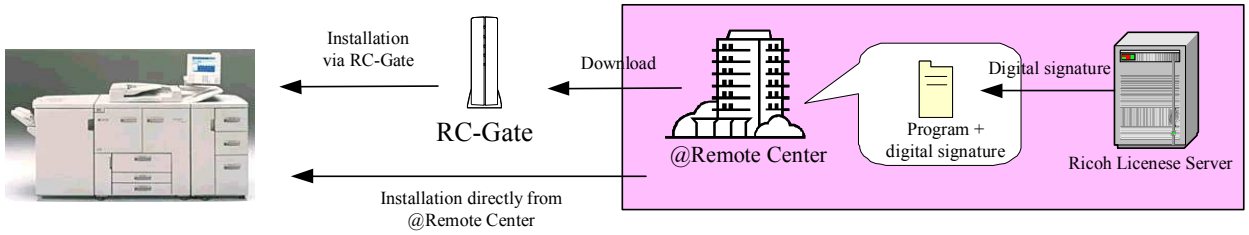
  The update is performed by a customer engineer (CE) in the field via a PC

  The update is performed using the @Remote function, normally by an individual with access rights to the @Remote Center GUI

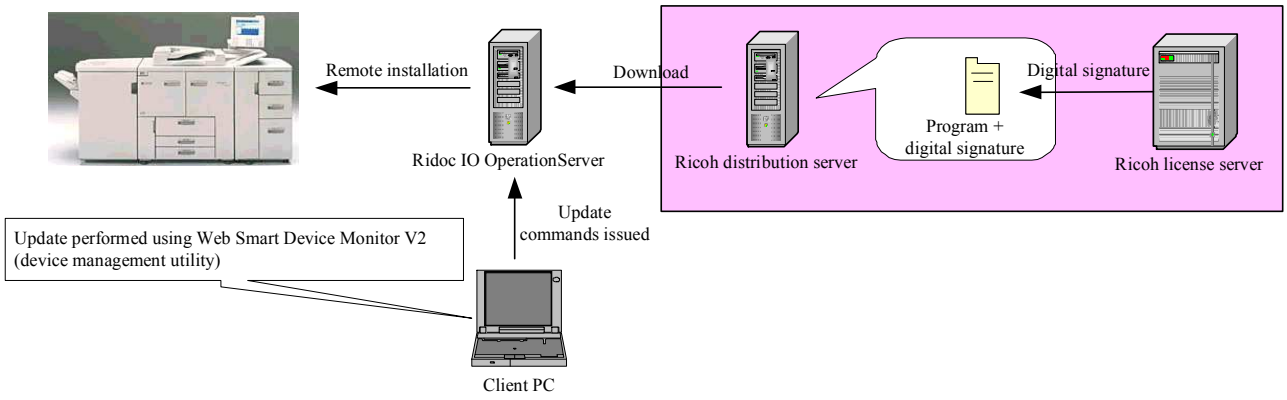
  The update is performed via Web SmartDeviceMonitor for Admin for Admin, usually by the end user


1. Check remote headers to confirm that a remote update is being requested
4. Files are sent
2. Verification of model and target machine functions (Copier, Printer, etc.)
3. Verification of firmware version
If MD1 ≠ MD 2
Update process is cancelled and new firmware is not installed
Program
Digital signature
5. Generate MD1 using SHA-1
MD 1
7. Compare MD and MD2
6. Decryption
Public key
MD 2
If MD1 = MD2
8. Firmware is overwritten with new files
Ricoh distribution server
Program + digital signature
Digital signature
Ricoh license server
Program
1. Generate MD using SHA-1
MD
Digital signature
2. Generate digital signature
Private key
3. Download
Client PC

Remote Firmware Installation Performed by a CE
(from a client PC)



Remote Firmware Installation using @Remote



Remote Firmware Installation via Web SmartDeviceMonitor for Admin for Admin (performed by the end user)

5. Authentication, Access Control

Authentication

- When enabled, User Authentication requires all users to go through a username and password-based authentication process before MFP/LP operations can be performed. This is true in cases where the user attempts to access MFP/LP functions via the operation panel as well as via a network connection.

  There are five types of User Authentication:
  - Basic Authentication
  - Windows Authentication
  - LDAP Authentication
  - User Code Authentication
  - Integration Server Authentication

- As the authentication server, the MFP/LP can be used for Basic Authentication, a Windows NT4.0 server, Windows 2000 server or Server2003 can be used for Windows Authentication, and an LDAP server can be used for LDAP Authentication. In addition, when "Integration Server Auth" is selected from the User Authentication menu, the MFP/LP connects to the actual authentication server via an Integration Server. In this case, the authentication is performed using the User Authentication functions of ScanRouter, ScanRouter Document Server, Web SmartDeviceMonitor for Admin or ScanRouter Web Navigator.
  Note: See "Windows Authentication, LDAP Authentication" and "Integration Server Authentication" diagrams below.

  Usernames:
  - Format: US-ASCII, WinLatin1, WinLatin2, WinCyrillic (except 2-byte characters used for display languages such as Chinese, Japanese, Taiwanese and Korean).
  - Length: Maximum 32 characters.
    Note: Although usernames longer than 32 characters are invalid, the input field will accept up to 128 characters in order to make the 32-character limit more difficult to surmise.

  Passwords:
  - Format: US-ASCII, WinLatin1, WinLatin2, WinCyrillic (except 2-byte characters in languages such as Chinese, Japanese, Taiwanese and Korean).
  - Length: Maximum 128 characters (general users), 32 characters (administrators).

- Before authentication at the MFP/LP operation panel can be performed, uses must be pre-registered in the MFP/LP. The communication path can be encrypted using SSL, however for environments that do not support SSL protocol, the password itself is encrypted using an encryption key specified by the Administrator. To do this, however, the Printer/Scanner option must be installed.

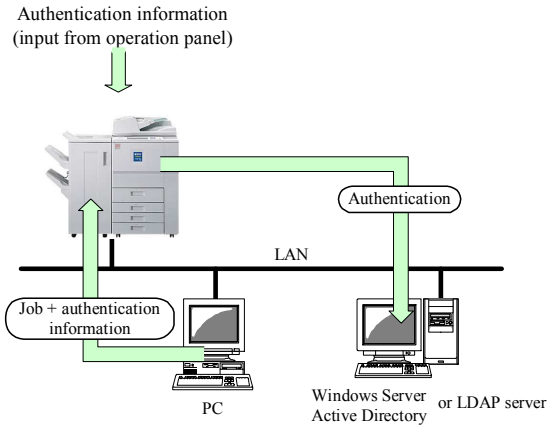
- To minimize the impact of brute-force attacks, the MFP/LP will delay sending the authentication results back to the originator in cases where authentication has failed.

- The information for performing the authentication of administrators is encrypted and then stored in the MFP/LP in non-volatile memory. Therefore, it is always possible to perform authentication on administrators even when a failure occurs with the MFP/LP HDD or one or more of the external authentication servers is down.

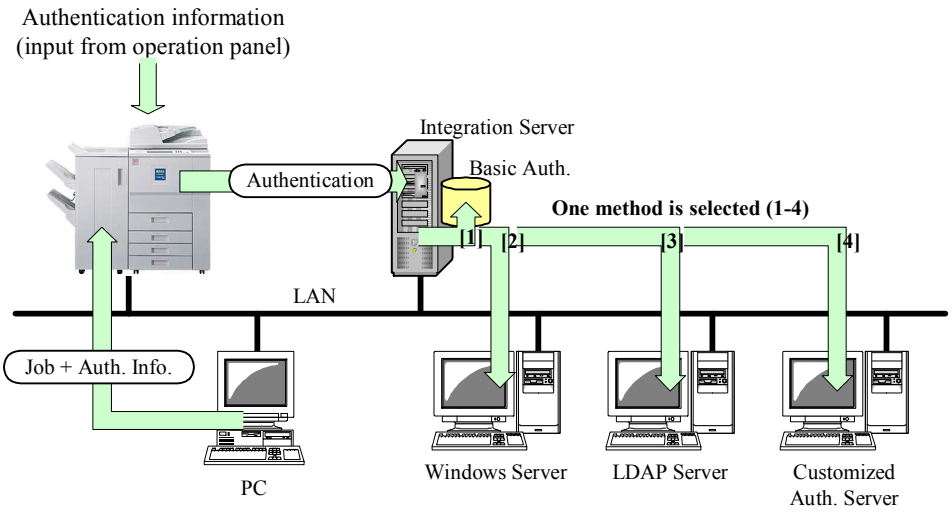
- With Windows Authentication, NTLM Authentication is performed with the specified domain controller, after which an attempt is made to establish an LDAP connection with the active directory. The email address, FAX number and GUID are then obtained for users who successfully clear the authentication. The same NTLM Authentication process is performed for LDAP Authentication as well, after which an LDAP search is performed to obtain the user's email address, FAX number and GUID.

Active sessions will expire under the following conditions:

- When the "Logout" button is pressed in User Tools
- When the "Logout" hard key is pressed (on MFPs/LPs that have this key)
- When the MFP/LP enters Low-power Mode or Energy Saver Mode
- After a pre-determined amount of time has passed (automatic logout)



Windows Authentication, LDAP Authentication



Integration Server Authentication

IC Card Authentication

Overview

- IC Card Authentication is provided to the field in the form of an optional IC card. The information necessary to perform the authentication functions described in section above (username and password, or serial number (IDm)) can be stored to this IC card and then used to authenticate MFP/LP users.

- One of two types of IC cards can be used: Those built to Ricoh specifications, and those build to Felica specifications (or containing a Felica chip). The former type uses the username and password, while the latter type uses the serial number (IDm) to authenticate the user.

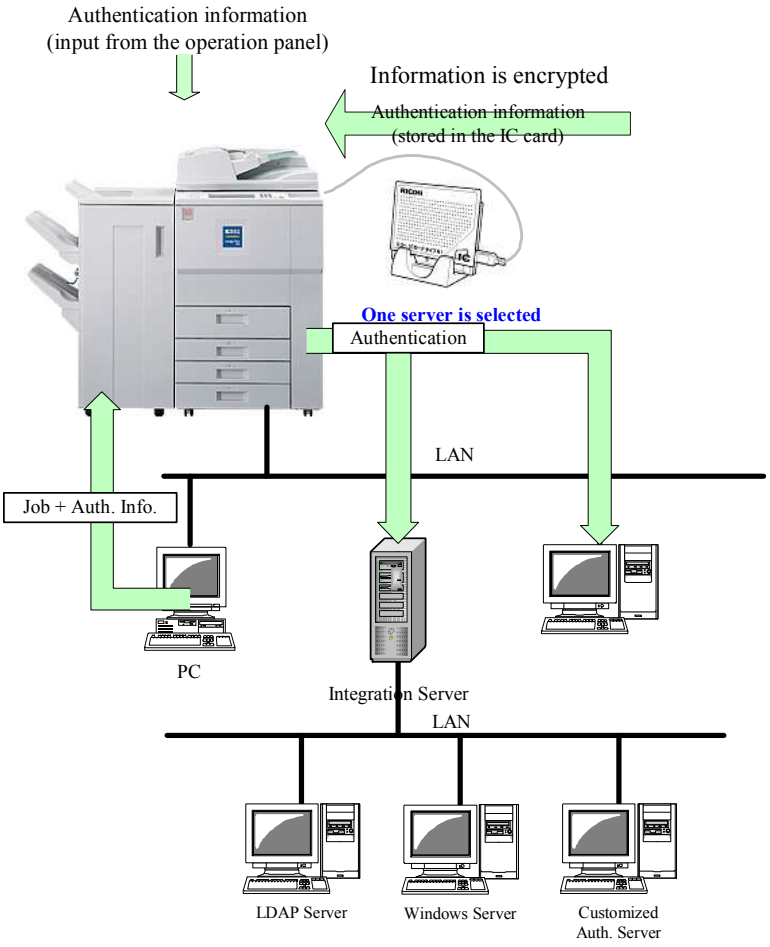
- To use this option, it is necessary to install the “ADK” (Authentication Development Kit), a local customization solution.

Data Flow

- IC Authentication using the username and password (Ricoh IC cards):
  When the IC card is placed in the reader, if it contains a function release code, the user will be prompted to enter this code in order to proceed with the authentication. The CSC compares the code entered with the one stored in the IC card, and if these two match, it then obtains the username and password stored in the card and begins the authentication process. If the IC card does not contain a function release code, the CSC simply reads the username and password stored in the IC card and begins the authentication process automatically.

- IC Authentication using the serial number/IDm (Felica cards or those containing a Felica chip): When the IC card is placed in the reader, the CSC reads the username and password stored in the card and begins the authentication process automatically.

Note: Standard Felica specifications do not support the use of function release codes.



IC Card Authentication

Access Control

Users logged-in as administrators are able to make changes to the following security-related settings:

- Access restrictions for individual users: Access to each principal MFP/LP function can be controlled for each individual user. In the case of Windows Authentication and Integration Server Authentication, it is also possible to set such restrictions for global groups as well as individual users.

- On MFP/LPs with email transmission applications, to prevent the impersonation of the user by a third party, it is possible to set the MFP so that the email address of the logged-in user is set as the "From" field whenever an email is sent. Users who do not have a registered email address would not be able to send email.

- It is possible to prohibit the sending of email to any address except those that have been approved. This is true for addresses that are entered manually as well as those registered in the Address Book.

- It is possible to prohibit unauthenticated users as well as general users from viewing or making any changes to the User Tools settings.

- An 8-digit protection code can be assigned to each individual Address Book entry to protect its contents, so that users cannot freely select addresses to send email and/or impersonate other users as the sender. If the code entered by the operator does not match the one in the MFP, no operations can be performed on the address. In addition, it is possible to create an access control list (ACL) for each individual Address Book entry and Document Server document at both the individual user and group levels.

6. Administrator Settings

In order to spread the risk of malicious operations by a single individual with administrator-level access rights, the MFP/LP allows the following five types of administrators to be registered.

- **Machine Administrator:** Manages the User Tools settings and ensures that the MFP/LP is always in good working order.
- **Network Administrator:** Manages the network-related User Tools settings and ensures that protections against illegal remote access are properly maintained.
- **Document Administrator:** Manages the document storage-related User Tools settings, access privileges for stored documents, and the stored documents themselves.
- **User Administrator:** Manages the user information stored in the Address Book, as well as the access rights to this information.
- **Supervisor:** Manages the passwords of the four administrators listed above.
- Each individual administrator is able to change their own username and password, however they are not able to change the usernames and passwords of other administrators.
- It is possible to assign two or more (or all) of the above titles to the same individual user.
- If the Supervisor forgets any of the passwords, the information cannot be retrieved by customer engineers or any other technical personnel. The only way to retrieve the information is to initialize the MFP/LP back to its factory shipment condition. If this is done, all of the user information, document data and settings performed since machine installation are initialized (erased).

7. Data Erase/Overwrite

Overview

- A wide variety of data is stored in MFP/LP memory both permanently and temporarily. The HDD stores data such as image data, email destinations, and Address Book data containing various types of user information. In addition, the NVRAM stores data such as User Tools settings, while the FCU stores FAX reception image data. Data stored on the magnetic media of the MFP/LP is normally "erased" by overwriting it with a fixed value (normally, this is performed once).

- However, in the case of a print/copy job, for example, although the MFP/LP completely erases the page location data (the storage location information necessary to access image data on the HDD), the image data itself remains in the temporary storage stored area of the HDD. The Data Erase/Overwrite feature, provided to the field as optional software stored on an SD card, renders this image data indecipherable. Even in the unlikely event that the HDD were removed from the MFP/LP, a third party would not be able to reconstruct the original data.

- In rare cases, performing the overwrite just once may not be enough to completely alter the magnetic pattern of the data to an indecipherable level, leaving the possibility of partial reconstruction of the original data. Because of this, the optional Data Erase/Overwrite feature employs the following methods, which ensure that data reconstruction is not possible.
  - The DoD method, developed and required by the U.S. Department of Defense
  - The NSA method, developed by the U.S. National Security Agency
  - The Ricoh randomized value method, a Ricoh-original method which overwrites data using randomly-generated values

  Note: The DoD and NSA methods automatically perform three passes, using a different pattern each time (the number of passes is unchangeable). The Ricoh randomized value method performs three passes by default, using a different set of randomly-generated numbers each time; however the number of passes can be set from 1-9. Comparing the DoD method, NSA method and Ricoh randomized value method (set at three or more passes), no single method is any safer than the other two. Under these conditions, all three methods render the data equally indiscernible. Regardless of which method is selected, the more passes are made, the more indiscernible the original data becomes (although performing more passes requires more time).

- Before the Data Erase/Overwrite option can be run on the MFP/LP, a service technician must perform the setup procedure. If the SD card is removed from the slot at any time after installation, the option will cease to function and an error message will be displayed on the operation panel, however the machine will continue functioning normally. Also, it is not possible to remotely verify whether or not the option is installed or actually running.

- To execute the overwrite the operator can choose from two options: "Auto Erase Memory" and "Erase All Memory" (detailed descriptions below).

Auto Erase Memory

- The main purpose of this feature is to automatically overwrite data stored to the processing region of the HDD, i.e. data that is saved to the HDD for purposes of MFP/LP internal processing only, of which users are normally unaware. Auto Erase Memory prevents this unnecessary data from remaining in the HDD by overwriting it as soon as it is no longer used by the MFP/LP.

- In addition, it is also possible to manually erase data that was intentionally saved to the HDD, such as Document Server documents.

Note: If the MFP/LP receives a request to perform a print job or other operation that requires writing data to the HDD in between the time the operator initiates the overwrite and the time the machine actually begins the overwrite, the area of the HDD in question may be used to store the incoming image data.

Erase All Memory

- This function overwrites the contents of every region of the HDD and initializes the contents of the NV-RAM and FCU. Since this operation makes it impossible to retrieve or reconstruct the contents of the HDD in addition to initializing the FCU data, Erase All Memory is primarily used at machine disposal or at the conclusion of a machine lease or rental contract. It is therefore necessary to back up the information mentioned above or send it to a PC for storage before executing Erase All Memory.

- By initializing the contents of the NVRAM to their default values, this feature prevents information that is unique to a particular installation environment from being released to third parties (e.g. IP address, control lists and other administrative information).

- The execution of this feature does not clear engine-related information such as the value of the total counter, or engine-related adjustment settings contained in SP mode and UP mode.

8. Data Protection

Protection of Address Book Data

- The tables below show the various types of data stored in Address Book entries as well as the operations that general users/groups, owners and user administrators can perform on this data. It is possible to assign general user access privileges to individual users as well as to groups. Users who have not been assigned any access privileges are not able to view the contents of Address Book entries.
- There are four levels of access privileges: View, Edit, Edit/Delete, and Full-Access. These settings can be changed by Group and User Administrators, users with Full-Access privileges and the user who registered the entry. User Administrators are also able to change user passwords.
- The data in the Address Book is stored in the HDD or SD card. This data can be encrypted before it is stored if the Printer/Scanner option is installed.

Access Privilege Management Structure for the Address Book

			General Users Groups	Owner of the Entry (User)	User Administrator
General Info.	Reg. No.	00001	R	RW	RW
	Name	Taroh Ricoh			
	Email address***1**	taroh@ricoh.co.jp	Use ACL		
	FAX No. ***1**	1234-5678			
	…	…			
Detailed User Info.	Login password***2**	**********	—		R
	Authent. Username***1**	Taroh			
	Authent. Password***1, *2**	**********			
	Protection Code	****			
Admin. Data	Login Username	Taroh	—	R	RW
	Authorized Usage	Copier			
	…	…			
ACL Information		00002=R--- 00003=RW-- 00004=RW-O 00005=RWDO …	Use ACL	RW	RW

Note:

***1**: This item does not appear in the Address Book on LP models.

***2**: This password can only be changed by users with Write privileges. As the user inputs the password, it is displayed as asterisks.

		View	Make Changes	Delete Entries	Change ACL Settings
R	View	Yes			
RW	Edit	Yes	Yes		
RWD	Edit/Delete	Yes	Yes	Yes	
RWDO	Full-Access	Yes	Yes	Yes	Yes

Access Privileges and Operations for the Address Book

Document Server Documents (MFP models only)

- The tables below show the various types of data stored in Document Server management files, as well as the operations that general users/groups, owners and User Administrators can perform on this data. It is possible to assign general user access privileges to individual users as well as to groups. Users who have not been assigned any access privileges are not able to view the contents of these files.
- There are four levels of access privileges: View, Edit, Edit/Delete and Full-Access. These settings can be changed by Group and User Administrators, users with Full-Access privileges and the user who registered the entry.
- A password can be assigned to each document (4–8 numeric characters long), ensuring that the document cannot be accessed unless the correct password is entered first. In addition, by enabling the Document Lock feature, the MFP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively. This setting can be enabled and disabled in System Settings by the Document Administrator.
- Every time a user logs in using Integration Server Authentication, the document protection setting in that user's Address Book stored in the MFP is automatically changed to "View (only)". Therefore if the user stores a file to the Document Server without changing the document protection setting for that document, or stores the file from an application that does not allow the setting to be changed, the user will not be able to edit or delete the document later. This automatic overwriting of the document protection setting in the MFP Address Book can be disabled for all users in Service Program mode (SP5-401-103).
- The Document Administrator can also change the passwords for individual documents without having to clear a password-based authentication process.

			General Users	Document Owner (User)	Document Administrator
General Info.	Document No.	00001	Use ACL	RW	RW
	Document Name	Meeting files			
	Thumbnails				
	Bibliographic Info.				
	Pg. 1 Image Data				
	Pg. 2 Image Data				
	・・・	・・・			
Detailed User Info	Document Password	********	—	W	W
ACL Information		00002=R--- 00003=RW-- 00004=RW-O 00005=RWDO ・・・	Use ACL	RW	RW

Access Privilege Management Structure for Stored Documents

		View Bibliog. Information	View Thumbnails	Printing, Sending	Edit Image	Delete Pages	Delete Doc.	ACL Settings
R	View	Yes	Yes	Yes				
RW	Edit	Yes	Yes	Yes	Yes			
D	Edit/Delete	Yes	Yes	Yes	Yes	Yes	Yes	
RWOD	Full-Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: *Deleting pages can only be performed on certain models.*

Access Privileges and Operations for Stored Documents

9. Additional Methods for Increased Security

In addition to the above, administrators can also perform the following settings as needed to provide additional security.

- Prohibit access to SP Mode without authorization from the user.
- Prohibit individual users from registering or making changes to Address Book entries.
- Change the complexity and minimum number of characters required to set a valid password (from 1 to 32 characters) for both Basic Authentication and Administrator Authentication. A password's complexity can be increased by requiring the use of two or more (or three or more) types of alphanumeric characters out of the four types available (capital letters, lower-case letters, numbers, and symbols).

Note: When users log in via the Integration Server, the MFP/LP does not check the password policy (e.g. length, complexity). Therefore, in such cases, the password policy must be managed by configuring the Integration Server settings.

10. Job/Access Logs

- Job logs and access logs for the principal machine functions in contain entries for job status-related events (initiation, completion, any changes during the job), while the access log contains entries for MFP/LP operational events (authentication, operations performed on documents, administrator operations). Therefore, not every single operational or status-related event is recorded in the log.

- Both logs are saved to the HDD by the LCS, and contain a date and time for each entry. By saving the data to the log along with the time and date of the operation performed, it is possible to then retrace the sequence of operations performed leading up to a machine failure. In addition, making it known that the time and date are recorded together with the operations can serve as a deterrent to unauthorized use.

- The specific events for which log entries are created vary slightly with each principal machine function. The events common to all principal machine functions are: SMC printout, log-in, log-out, storage or deletion of a file in the Document Server (MFP HDD), deletion of all Document Server documents in a single operation, HDD format, deletion of all log entries in a single operation, and changes to log settings. For the events that are unique to each principal machine function, please refer to sections below.

- It is then possible to have the MFP/LP send the log data to Web SmartDeviceMonitor for Admin (a log data server utility) whenever any of the events described above occurs, after which the data is stored in an MSDE or SQL Server database. Only users who are registered with an administrator-level User Account in Web SmartDeviceMonitor for Admin can access the contents from a Web SmartDeviceMonitor for Admin client station. In addition, these administrators are the only persons who can perform any changes to the log data transfer settings.

  The log data is encrypted before being saved to the HDD, which prevents any illegal acquisition or alteration of the data through unauthorized access to the HDD. In addition, the encrypted data is sent via the LCS and GWWS to Web SmartDeviceMonitor for Admin over an SSL connection.

- Before log data can be transferred from the MFP/LP to Web SmartDeviceMonitor for Admin, it is necessary to assign MFP/LP administrator types 1-4 described in Administrator Settings to a single account, and then create an administrator-level Access Account in Web SmartDeviceMonitor for Admin with the same name and password. It is also necessary to enable the settings for log data sending in the MFP/LP and in Web SmartDeviceMonitor for Admin.
  Note: For more information on the transfer of this data, please refer to Netfile.

- The MFP/LP does not allow any changes to be made to the log data itself, i.e. the data can only be transferred to Web SmartDeviceMonitor for Admin in an unaltered, encrypted state. Therefore, the data cannot be overwritten or modified in any way, even by those with administrator-level access rights.

- When the log reaches its capacity, the oldest entries are then overwritten one by one by each new entry. To ensure that this data is not lost, it must be sent to Web SmartDeviceMonitor for Admin before it is overwritten. As mentioned above, the MFP/LP sends the data to Web SmartDeviceMonitor for Admin only when an operational or access event has occurred.

Note: With MFP/LPs that do not have an HDD installed, the log data is stored in volatile RAM. The data is therefore erased when the MFP/LP main power is turned off. In addition, since the RAM capacity is not as large as that of the log area in the HDD, the oldest log entries will be overwritten sooner.

- The time it takes for the log to reach its capacity depends on the log capacities and rate at which the events (log entries) are recorded.

➢ **Job log**

Capacity:

With HDD: 2000 entries

Without HDD: 500 entries

Time to full condition:

With HDD: 2000/N minutes

Without HDD: 500/N minutes

Note:

- One job = one log entry
- N = Average number of jobs (log entries) generated in one minute

Example: An HDD is installed, and the MFP/LP receives an average of five (5) jobs per minute.

2000 / 5 = 400 minutes (6 hours, 40 minutes)

- **Access log**

  Capacity:

  With HDD: 6000 entries

  Without HDD: 500 entries

  Time to full condition:

  With HDD: 6000/M minutes

  Without HDD: 500/M minutes

  Note:

  - One job = one event
  - M = Average number of events (log entries) generated in one minute

  Example: An HDD is installed, and an average of eight (8) events occurs per minute.
  6000 / 8 = 750 minutes (12 hours, 30 minutes)

11. Capture (MFP Models Only)

Overview of Capture Operations

- When a user makes a copy or performs any of the operations listed below, the Capture function sends a copy of the image over the network to ScanRouter, after which it is forwarded to its final destination, ScanRouter Document Server.
- This function can be used to back-up images, or as a means of maintaining records of MFP usage for each individual user.
- It is possible to enable/disable the function. The type of capture can be set to Auto, Manual, Compulsory (Name Fixed), Compulsory (Name Available) or Do Not Capture. Other settings are described in detail below.
- When sending to ScanRouter, the MFP attaches a copy of the captured image's meta-data (i.e. owner data, usage data and Job Log ID).

Operations that Generate Captured Images

- Images are captured and sent to ScanRouter whenever any of the following operations are successfully completed. Once the main setting is enabled, the capture will occur automatically if Auto or Compulsory is selected, and only when the user specifies if Manual is selected.
  Note: The MFP itself is able to capture incoming FAXes as well, but ScanRouter currently does not support this.

Function	Operation
Copier	Copy job
	Copy job + storage to HDD
Document Server	Storage to Document Server
	Printing out of Document Server document
FAX Transmission	Regular FAX transmission
	Regular FAX transmission + storage to HDD
	Storage of regular FAX file to HDD for later transmission
	Transmission of FAX transmission file stored in HDD
	Printing out of FAX transmission file stored in HDD or SAF memory
	LAN FAX transmission
	Storage of LAN FAX file to HDD for later transmission
	Transmission of LAN FAX file stored in HDD
	Printing out of LAN FAX transmission file stored in HDD or SAF memory
Printer	Print job (incl. Normal Print, Locked Print, Sample Print)
	Storage of Printer file to HDD
	Printing out of Printer file stored in HDD
	File printed out with Remote Print
Scanner	Forwarding
	Forwarding + storage to HDD
	Storage of scanned image
	Forwarding of stored file
Desk Top Editor For Production	Restoring a previously downloaded file from Desk Top Editor For Production to the MFP HDD.

Capture Settings

- ScanRouter is used to program all settings for the Capture function.

- The following are the principal settings for this feature. Except for Compulsory, these settings do not require Administrator-level access rights to be changed.

1. Principal settings:
   - The Capture function can be enabled or disabled.
   - It is possible to select Auto, Manual, Compulsory (Name Fixed), Compulsory (Name Available) or Do Not Capture.

     Note: If "Compulsory (Name Fixed)" is selected, the MFP will not display the owner name settings screen.

ScanRouter setting:	Display owner name screen on MFP panel:	Automatically capture the image:	Programmable by non-Administrator users:
Compulsory (Name Fixed)	No	Yes	No
Compulsory (Name Available)	Yes	Yes	No
Auto	Yes	Yes	Yes
Manual	Yes	No	Yes
(Do Not Capture)	No	No	No

2. Other settings
   - Owner name selection

     The Owner Name is used by ScanRouter and ScanRouter Document Server to keep records of which operator performed which operation for each incoming captured image. This setting controls whether or not to permit multiple owners to be assigned to the same document.

   - Default owner name

     This is the default name that will be used as the Owner Name for cases in which the user did not set one.

   - Control of "Public" status setting

     This setting controls whether or not to permit the user to assign the captured document a "Public" status, which would make the document viewable to all authenticated users after being delivered to ScanRouter Document Server.

Security Considerations

- Three transfer protocols are available for sending captured documents to ScanRouter: FTP, HTTP and HTTPS. Protocol selection is based on the settings programmed in ScanRouter.
- In order to use HTTPS, it is necessary to install ScanRouter EX or later and then enable the appropriate settings for encrypted communication. In addition, the operator can also set the machine to authenticate the target ScanRouter server. To do this, it is necessary to pre-register the digital certificate of the trusted ScanRouter server in the MFP.

Captured Documents and Log Data

- A Job Log ID is embedded in every captured document. If the Job Log function was enabled at the time the document was captured, it is then possible to use this ID to view the contents of the corresponding log entry.

Note: This is not possible for FAX documents.

12. Principal Machine Functions

Copier (MFP Models Only)

Overview of Copier Operations

- When a copy job is initiated, the scanning engine scans the original and forwards this data to the controller to be printed out from the printing engine. If “Store File” is selected at this time, the image data is also stored in the HDD.

- The Document Server function can also be used to scan images and store them directly to the HDD without printing them out, as well as to print out documents already stored in the HDD. In addition, a password can also be assigned when scanning a document for storage to the HDD, requiring the operator to input the correct password to print out the document.

- User Codes can be enabled to restrict access to the Copier function.

Data Flow

- A copy job is initiated from the Copier function, which sends a job start command to the ECS. In turn, the ECS instructs the scanner engine to begin scanning and the MCS to secure the necessary amount of memory in the volatile RAM (Image Memory RAM). The scanned image data is then temporarily stored in the Image Memory by the IMH, after which the ECS instructs the IMH to retrieve the data and send it on to the printing engine. The data is printed out according to the specified number of pages, after which the ECS erases the image data via the MCS.

- When scanning documents for direct storage to the HDD or for simultaneous storage and copying, the data is sent via the MCS and saved to HDD memory.

- The Document Server screen displays a list of all MCS-managed files that the Copier function is able to print out (i.e. all documents saved to the Document Server except Scanner files). When the operator selects a document from this list and presses the print button, the Start command is sent to the ECS and the document is printed out by the Copier function.

- The Copier function keeps track of how many copies have been made in each copy mode by storing these values in the non-volatile RAM (NV-RAM). These counters are incremented after each page is printed and at the conclusion of every job. These values can be viewed on the operation panel from inside SP mode or in machine service reports.

Data Security Considerations

- Since the page location data is erased at the conclusion of every copy job, it is not possible to perform a job re-print on the same data. In addition, since the Copier function itself does not have any external I/F and does not perform any data exchanges or communication with external devices, it is not possible for any illegal external data to be introduced through the Copier function.

Protection of Copy Jobs in Progress

- When User Authentication is enabled, if one user attempts to cancel a copy job in progress that was initiated by a different user who had logged out before the end of the job, the MFP will prompt the operator for the username and password of the user who originally initiated the job. The only individuals who can successfully cancel the job are the Machine Administrator and the user who initiated the job. Also, the Machine Administrator always has the ability to perform operations on copy jobs in progress (e.g. job cancel).

Protection of Document Server Documents

- When User Authentication is enabled, it is possible to assign specific access privileges to individual documents when storing them to the HDD, which limits what operations can be performed on them (e.g. View, Edit, Delete, and Full-Access).

- Users with View privileges can view, duplicate and print out documents but cannot delete or make any changes to the document (incl. filename). Users who have Full Access privileges can perform all operations on the document including viewing, printing, duplicating, editing and deleting, as well as making changes to the document's access privileges settings. Users who have not been assigned any of these access privileges cannot perform any of these operations, and are also prohibited from selecting documents in the document list screen.
  Refer to Document Server Documents (MFP models only) for details on the Document Lock feature.

Protection of Copier/Document Server Features

- When Machine Administrator Authentication is enabled and the Menu Protect setting in Copy/Document Server Features is set to "Level 2", changes to the Copy/Document Server Features can only be performed by the Machine Administrator. With a setting of "Level 1", users are able to change a select number of items, while a setting of "None" allows users to change all items.

Restricting the Available Functions for Each Individual User

- When User Authentication is enabled, it is possible to then allow or prohibit the use of specific Copier functions for each individual user. For example, with color products, it is possible to allow or prohibit the use of B/W, full-color, two-color and single-color modes for each user. Therefore, if a user were assigned restrictions that limited him or her to B/W copies, even after having successfully logged in, they would not be able to make color copies.

- In addition, it is possible to prohibit Full Color printing and instead enable Auto Color Detection, which ensures that the MFP only uses black toner to print out black and white originals. As this minimizes the amount of color toner consumed, this has the added benefit of reducing costs.

- It is also possible to increase the level of security by using the above features in tandem with an external charge device or key counter. This is because operators would not only be prompted to enter a user name and password, but would also be required to clear the usage restrictions imposed by the external charge device or key counter itself (card, currency, etc.).

Job/Access Log Data Collection

- An entry is added to the job log for each individual job, containing information on the job settings (e.g. simplex or duplex, paper size), completion status (whether completed successfully or not) and user identification (in cases where User Authentication was enabled).

- Whenever the optional Copy Data Security Unit detects one of the embedded patterns selected with the Copy Data Security feature (section 3.3), an entry is added to the access log.

- The log data is saved to the HDD via the LCS. It is possible to set the MFP to send the job log data stored in the HDD to Web SmartDeviceMonitor for Admin whenever a job has been performed.

- The job log data can be permanently erased from HDD memory from inside SP (Service Program) Mode.

Print Backup

- After a job is performed, it is possible to store a copy of the image data in the HDD (via the MCS), and then use the Netfile function to retrieve this data to Desk Top Editor For Production. For more on this data flow, see Data Flow.
- The supported file formats for this operation are: JPEG2000, JPEG, TIFF, PDF (single-page) and PDF (multi-page). The file format must be selected from the MFP operation panel before the Copy job is started.
- When sending the file in PDF format, it is possible to pre-set the password necessary to open the encrypted PDF data at the PC side, the password necessary for changing the document's access level, and other security settings associated with the document (e.g. printing out, editing, copying).

13. Printer

Overview of Printer Operations

- The Printer function can be divided into main processes: 1) Converting the printer language data received by the MFP/LP into image data, and 2) Printing out this image data onto the paper in accordance with the specified job settings. The former is performed by the printer language processing subsystem, while the latter is performed by the printing subsystem.

- Once the data sent from the host computer is accepted, and the processing subsystem begins processing the new print job, a print job log entry is created (temporary entry). The entry is registered as soon as the job is completed.
  Note: The Document Server and all related Printer functions described below are supported by **MFP models only.**

Data Flow

Printing Unencrypted Image Data

- As stated above, the printer language-encoded data sent from the host computer is interpreted by the language processing subsystem, after which it is converted into image data and then stored temporarily in the Page Memory in binary bitmap format. Once this is done, the data is compressed in Ricoh original compression format, and stored in the HDD page by page. If the MFP/LP does not have an HDD, the compressed data remains in the Page Memory and is treated the same as data written to the HDD.

- When Spooling is enabled, the incoming data is stored directly to the spooling area of the HDD. Following this, the data is sent to the language processing subsystem, where it is interpreted and converted to image data page by page. Before it is printed out, the spooled data can be deleted from the “Spool Printing” list in WebImageMonitor, or “Spooling Job” list on the MFP/LP operation panel. The data is developed page by page in the order in which it was converted (beginning from page 1), however the actual printing order of the pages may differ depending on the job settings received from the printer driver (e.g. duplex vs. simplex, usage of Booklet or Stapling features, etc.).

- When Image Spooling in enabled, all pages of the incoming data are converted to image data and then stored to the HDD. Once this is completed for all pages, the data is then sent to the printing engine for printing out.
  Note: The order in which jobs are printed out is same whether Image Spooling is enabled or disabled.

- From the printer driver, it is possible to select the following printing methods: Normal Print, Sample Print, Locked Print, Hold Print, Stored Print, Store and Print, and Save to Document Server. The data processing flow varies depending on the method used since some operations are not supported with some printer languages (see below).

- With Normal Print, the page location data for the image data stored in the HDD is erased at the conclusion of the print job or when the main power is turned off. When Sample Print is selected as the job type, the document will remain in the HDD as a Sample Print document even after the sample set is printed out. Additional sets of this document can then be printed out from WebImageMonitor or the MFP/LP operation panel, after which the page location data is deleted at the conclusion of the job.

- When Locked Print or Hold Print is selected as the job type, the image data is saved directly to the HDD as a Locked Print or Hold Print document, without being printed out. Locked Print and Hold Print documents stored in the HDD can then be printed out from WebImageMonitor or the MFP/LP operation panel, after which the page location data is deleted at the conclusion of the job.

- When Stored Print is selected as the job type, the image data is saved directly to the HDD as a Stored Print document, without being printed out. When Store and Print is selected as the job type, the image is saved to the HDD and is also printed out. Just as with the above, the documents stored in the HDD can also be printed out from WebImageMonitor or the MFP/LP operation panel, however these documents remain in HDD memory even after the conclusion of the print job.

- When Save to Document Server is selected as the job type, the image data is stored directly to the HDD as a Document Server document, without being printed out. The necessary bibliographic information for the image data is stored in the HDD along with the image data itself. The bibliographic information is part of the print management data, and includes information such as the page size, paper type and number of sets.

  Document Server documents can be printed out from the MFP operation panel or from WebImageMonitor, after which they remain stored in the HDD. In addition, the documents remain stored in the HDD even if the main power is turned off.

- When Normal Print is selected as the print job, the print management data[*1] for the image data stored in the HDD is stored in volatile RAM memory in Ricoh original format. It is erased at the conclusion of the job, together with the page location data.

- When Sample Print, Locked Print, Hold Print, Stored Print, Store and Print, or Save to Document Server is selected as the print job, the necessary bibliographic information for the document is stored in the HDD along with the image data itself. This information and data is preserved even when the machine main power is turned off.

- The user ID can be registered in the printer driver UI, which machine operators can then use as a unique marker for documents to differentiate them from one another. Once a user ID is registered, it is used for the Sample Print, Locked Print, Hold Print, and Stored Print printing methods, and also appears in the printing history. In addition, it is also possible to set the passwords for Locked Print and Stored Print documents as well as the username and password for Document Server documents.

- Once the necessary username and password have been set in the printer driver, it is possible to perform User Authentication when sending data to the MFP/LP. The username and password are sent along with the printing data as authentication data. If authentication fails, the printing data sent to the MFP/LP is destroyed and the job is cancelled.

- The print job history is stored in volatile memory and is therefore deleted when the MFP/LP main power is turned off. The information stored includes the username, number of pages, the time the print job was performed, and job status/results. The print job history can be accessed from SmartDeviceMonitor for Client, which retrieves the information via a Ricoh-original MIB over an SNMP connection.

[*1]: The “print management data” is managed and maintained by the Printer function itself, and contains information such as the size of the paper for printing, job settings (simplex or duplex, etc.) and general job data (time, username, etc.). This is not the same as the “page location data” for the image data stored in the HDD.

Printing Encrypted Image Data

- With PDF Direct Print, it is possible to print out an encrypted PDF file. The password is registered in the Printer function via WebImageMonitor or the MFP/LP operation panel, or is set inside DeskTopBinder (incl. the Function Pallet). When the printer receives the file, the printer language processing subsystem (PDF interpreter) temporarily stores the file directly to the HDD. Once the file is recognized as an encrypted PDF file, the password registered in the MFP/LP is compared to the password sent along with the file. If they do not match, the data itself will not be decrypted correctly, causing an error to occur and the job and data to be erased. If they do match, the data will be decrypted correctly. After this, the decrypted data is converted to image data, stored to the HDD and then follows the normal process described above.

- When Spooling is enabled, the incoming encrypted data is stored directly to the spooling area of the HDD. Following this, the first page of the data is then sent to the PDF interpreter to be interpreted.

- It is also possible to set the MFP/LP to prohibit the printing of PDF files. PDF files for which this setting is used cannot be printed out when received by the MFP/LP, as the MFP/LP resets the job and deletes the data.

Data Security Considerations

Printing Unencrypted Image Data

- The language processing subsystem only allows data in legal format to be processed. In the event that illegal data is received, the subsystem will declare an error and cancel the processing session.

- When User Authentication is enabled, the MFP/LP will only accept printing data that contains a username and password (or User Code in the case of User Code Authentication) that matches those of a pre-registered user. Any such data is destroyed, preventing the introduction of illegal data. When the Printer's authentication mode is set to Simple Authentication, the MFP/LP does not perform authentication on data sent from users that have been given "Guest" status.

- The password necessary for authentication is encrypted before the printer driver sends it to the MFP/LP. When performing the encryption, it is possible to use a key that is common to both the driver and the MFP/LP, known as the driver encryption key. It is also possible to encrypt the password using Simple Encryption, which does not use the driver encryption key. If the “Permit Simple Encryption” setting in the MFP/LP is disabled, the MFP/LP will only accept passwords that have been encrypted using the driver encryption key. Therefore under these conditions, even when the MFP/LP receives data with passwords encrypted using Simple Encryption, the job will be reset and the data will not be printed out. It is therefore recommended to use a stronger encryption method, which ensures that a third party attempting to tap into the communication path will not be able to surmise the actual password and impersonate the password holder.

- In addition the printing data itself, it is also possible to encrypt the communication path by selecting “IPP over SSL” as the network communication protocol.

- Although any authenticated user can view the “Spool Printing” list (WebImageMonitor), printer job history and error log, it is possible to display other users’ information in the in the form of asterisks (“****”).

- When Locked Print is selected as the job type, and the operator wishes to print out a Locked Print document stored in the MFP/LP from the operation panel or WebImageMonitor, it is necessary to enter a password before the job can be performed. If this password does not match the pre-registered password, the operator is not allowed to retry. This prevents illegal access to Locked Print documents.

- When User Authentication is not enabled, it is possible to view the list of Locked Print documents created by all users, however all filenames are displayed as asterisks (“****”). When User Authentication is enabled, the user cannot view any information on this list until authenticated. However, even after successfully logging in, the user can only view a list of his or her own Locked Print documents (the filenames for which are displayed as is, without asterisks).

- Stored Print or Store and Print documents in the HDD can be printed out from WebImageMonitor or the MFP/LP operation panel, as described earlier, and can be protected with a password. If a password has been assigned to the document, the operator will be prompted when attempting to print it out. The document cannot be opened unless the correct password is entered, which prevents illegal access to the document.

- It is possible to make a Stored Print or Store and Print document available for printing out by any authenticated user by selecting “Share” in the printer driver’s Advanced Options settings when the job is sent. It is also possible to change the access privileges setting for the document from WebImageMonitor. Normally, this is set in the printer driver to grant access to either all authenticated users or to the creator of the document alone. However the user can change this setting to grant access to specific user(s) or group(s).

- In addition, it is possible to enable the Document Lock feature, whereby the MFP/LP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively. This protects documents from attempts to crack the password via brute-force attacks. The operator can also change the password at any time, making it much more difficult to surmise. This is particularly helpful in cases where documents are stored in the HDD for extended periods of time.

- The language processing system is only capable of processing legal data in pre-defined formats. Therefore, even in the case that illegal fonts or firmware were downloaded to the MFP/LP on-board memory, such data could not be executed as a program nor be processed by any of the MFP/LP’s internal modules.

Printing Encrypted Image Data

- As stated above, PDF Direct Print handles the sending of encrypted PDF files. The main use of this function is for sending encrypted PDF files in cases where it is not possible to encrypt the communication path itself. Once the password for opening the file has been programmed from the MFP/LP operation panel or from WebImageMonitor, it is possible to then safely send the printing data over the communication path. Even if the PDF file sent as printing data were intercepted on its way to the MFP/LP, the contents of the data are secure since the data is already encrypted.

- As stated above, the password for opening the file can also be programmed from inside DeskTopBinder. Since this allows the user to assign unique passwords to each individual PDF file, this function can be used to distribute confidential documents. Since both the printing data and distributed PDF file itself are sent along the communication path in an encrypted state, their contents are secure. Even if the PDF file were intercepted at the PC or server point, the contents of the file cannot be accessed. In addition, the password itself is also protected since it is encrypted using the group password already programmed in DeskTopBinder.

- As stated above, the PDF interpreter cross-references the password programmed in the MFP/LP with the encrypted password sent from the PC, and destroys the incoming data when these passwords do not match. In addition, the incoming data is also destroyed if accompanying information alerts the MFP/LP that printing of this file is prohibited. Since the MFP/LP will reject such data, it is not possible for the data to introduce any illegal programs or be processed by any MFP/LP modules.

14. Scanner (MFP Models Only)

Overview of Scanner Operations

- Depending on the settings selected, the Scanner function does one of the following:
  1) Saves the scanned image to the HDD and then sends it via the network I/F as an email (via an SMTP server), to a folder (FTP server, client PC with Windows 98 or newer), or forwarding server (via ScanRouter),
  2) Saves the scanned image to the HDD alone without forwarding it, or
  3) Temporarily stores the image to the HDD and then forwards it to one of the destinations mentioned above.

  With the third option, the page location data for the data temporarily stored to the HDD is deleted once the destination receives the transmission, or after the maximum number of transmission attempts has been reached.

- With the TWAIN I/F, the TWAIN driver can initiate a scanning job under specified conditions from a network-connected client PC, after which the image is sent back to the TWAIN driver.

- Access to the Scanner function itself or to specific features can be restricted with the use of User Authentication, the Available Functions settings for each individual user, and an external coin/card operated device. Use of the TWAIN feature is only allowed after a crosscheck with the User Code, User ID and password pre-programmed in the TWAIN driver U/I.

- Operational log entries are created for both scanning and forwarding jobs. The forwarding results can be printed out or viewed directly from the operation panel (“Scanned File Status”). These results are stored in non-volatile memory, i.e. the data is preserved even after the MFP main power is turned off.

Data Flow

- The raw image data sent to the RAM managed by the IMH goes through MH/MR/MMR/JPEG compression or is left uncompressed, depending on the operator’s settings. TIFF headers are attached to all data except JPEG-compressed files. The data is then sent over the network in a commonly used image file format. In addition, it is also possible to convert these files to multi-TIFF or PDF format before they are sent.

- When sending an email from the MFP via the SMTP server, the operator can either send the scanned image as a file attachment, or send a text-only email that contains the URL for accessing the image in the MFP HDD. Using this URL, the operator then accesses the image via DeskTopBinder or Desk Top Editor for Production.

- When authenticating with User Codes, the User Code data is sent from the TWAIN driver in binary format (unencrypted). However when using User Authentication with the TWAIN driver, the password is encrypted before being sent. In addition, the password set from the MFP operation panel for accessing Document Server documents is not sent to DeskTopBinder or Desk Top Editor for Production. This password is only used for authentication when downloading the requested Document Server documents to these PC applications, or for access control with remote forwarding.

Data Flow Security Considerations

- Forwarding operations are unidirectional, sending image data to pre-programmed email addresses, folders and forwarding servers only. Since there is no receiving aspect, it is not possible for the Scanner function to receive any illegal data from an external interface.

- When sending image data to an SMTP server, it is possible to introduce an authentication process at the POP server before making the connection to the SMTP server (POP before SMTP), and at the SMTP server itself (SMTP authentication).

- When sending image data to an SMTP server or Windows PC (SMB), it is possible to encrypt the password using a DIGEST algorithm. When sending the file in PDF format, it is possible to pre-set the password necessary to open the encrypted PDF data at the PC side, the password necessary for changing the document's access level, and other security settings associated with the document (Printing, Changes, Content Copying and Extraction).

- The TWAIN driver will not process any binary data that does not conform to the predetermined protocol of the command interface. The supported protocols are SNMPv1, v2 and v3. When using SNMP v3, it is necessary to use the TWAIN V4 driver. In order to utilize the authentication features with the TWAIN V4 driver, the operator must first set the necessary authentication information in the authentication tool that comes with the driver.

Protection of Data when Performing Scanning and Sending Operations

It is possible to set the MFP or related software to perform the following operations:

- Require user identification when sending to a forwarding server. By requiring the operator to select from pre-registered email destinations and then input a protection code, it is possible to protect against sender impersonation.
- Require user ID and password authentication before data is forwarded to an SMTP server or folder (Basic Authentication). This makes it possible to control the sending of data for each registered user.
- Require a numerical protection code (up to 8 digits long) when the operator selects a document stored in the MFP for sending, which protects against unauthorized email sending.
- Perform user access restrictions and further prevent any impersonation of the sender:
  When User Code Authentication or Basic Authentication is enabled, and a successfully logged-in user performs a sending operation, this user is automatically set as the sender of the email. If this user does not have an email address, it is not possible to send the email.
- Limit the sending of email to destinations that have already been programmed in the MFP. This can be done using the “Restrict use of destinations” setting of the Extended Security feature.
- Require user ID and password authentication when attempting to retrieve email addresses from an LDAP server.
- Set the MFP so that it is not possible to register email addresses in the MFP, whether obtained from an LDAP server or entered manually.

- In order for the MFP Scanner to retrieve the address book data of individual registered users from the forwarding server, Basic Authentication must be enabled at the MFP and the forwarding server software must be ScanRouter V2/EX or later. In all other cases, the MFP Scanner is either able to obtain shared address book data only via port 3670 (Basic Authentication disabled, all versions of ScanRouter), or is not able to obtain any data at all (Basic Authentication enabled, ScanRouter V1). The data obtained from the forwarding server is then deleted at the MFP when the user logs out.
  Note: Administrators cannot perform these operations.

- By enabling Basic Authentication, it is possible to protect the destination information. For each destination, it is possible to assign an access level to each registered user (View, Edit, Delete, and Full-Access). Users who have View privileges for a particular destination can select the destination for forwarding, but cannot edit or delete the data. Users who have Full-Access privileges can perform all functions including sending to the destination, editing and deleting data, and making changes to access privilege settings. Users who have not been assigned any of these access privileges cannot even view the destination list. Even when all of the above restrictions are enabled, User Administrators have Full-Access privileges for all registered destinations. However since User Administrators cannot use the Scanner function, they are not able to send any data.

- When logged in with Basic Authentication, users are able to perform operations with either the forwarding feature or the TWAIN driver feature, not both. However with User Code Authentication, there are conditions in which one operator can utilize the Scanner via the TWAIN driver even while another operator is already logged in from the MFP operation panel (i.e. before the user logged in from the operation panel actually initiates a job).

- With the TWAIN feature, the user is logged out automatically as soon as scanning is complete. Also, the authenticated user and Machine Administrator are the only individuals who can interrupt a scanning job in progress. When the Stop key is pressed to interrupt the job, the MFP prompts the operator with the authentication dialog.

Protection of Document Server Documents

- When Basic Authentication is enabled, it is possible to assign access privilege to individual documents when scanning them for storage in the Document Server (View, Edit, Delete, and Full-Access). These access privileges are applied even when accessing the document from DeskTopBinder or Desk Top Editor for Production. Users who have View privileges can both preview and send a document, but cannot delete or make any changes to the document (including the filename). Users who have Full-Access privileges can perform all functions including previewing, sending, editing and deleting the document, as well as making changes to the access privileges settings. Users who have not been assigned any of these access privileges cannot perform any of these operations, and are also prohibited from selecting documents in the document list screen. Even when all of the above restrictions are enabled, Document Administrators have Full-Access privileges for all registered documents. However since User Administrators cannot use the Scanner function, they are not able to send or store any data.

- It is also possible to assign a password to individual documents when scanning them for storage in the Document Server. After this, the document cannot be sent unless the correct password is entered. Additionally, when the Document Protect feature in System Settings is enabled, the MFP will deny any attempt to access a given document if an incorrect password is entered ten times consecutively.

Protection of Sending Results and Status Information

- When Basic Authentication is enabled, authenticated users are only able to view the sending results for the jobs that they performed. Results for jobs that other users performed are displayed as asterisks ("***"), preventing any leakage of information to third parties. The information is hidden in this way when displayed on the LCD, as well as when the results report is printed out. When Basic Authentication is enabled, entries in the sending results report can only be deleted by the user who performed the particular job. This prevents operations from being performed on these entries by third parties.

- Even when all of the above restrictions are enabled, Machine Administrators have Full-Access privileges for all log entries. Machine Administrators are able to view and print out all entries.

- By default, the sending results log is automatically printed out when the maximum number of entries has been reached. It is possible to disable the automatic printing out of this log in Scanner Features, which ensures that the information on the log is not leaked to unauthorized third parties, and also allows administrators to keep a record of every transmission job performed. However, when the log reaches the maximum number of entries (with this setting disabled), the MFP displays an alert message to this effect and gives the Machine Administrator the option of printing out the log.

Protection of the Scanner Features Settings

- When User Authentication or Administrator Authentication is enabled, users and administrators must be authenticated before they are allowed to make any changes to the settings in Scanner Features. When Machine Administrator Authentication is enabled and the Menu Protect setting is set to "Level 2", changes to the Scanner Features settings can only be performed by the Machine Administrator. With a setting of "Level 1", users are able to update the delivery server destination list as well as change the file compression and email display language settings (System Settings). With a setting of "None", users are able to change all items in Scanner Features.

- As explained above, the email forwarding feature sends data from the MFP to external destinations via the network. By changing the network traffic-related settings, which can only be performed by Network Administrators, it is possible to prohibit or limit the conditions under which emails from the MFP are actually forwarded to their destinations.

Data Stored in the Job Log

- An entry is added to the job log for each individual job performed, and contains information on the job settings (e.g. scanning settings, destinations), completion status (whether completed successfully or not) and user identification (in cases where User Authentication was enabled). The information is sent to the HDD via the LCS. For more details on job and access logs, please refer to Job/Access Logs.

Terminology

SMTP (Simple Mail Transfer Protocol) [RFC2822]: A protocol used for the transmission of email over the Internet.

SMTP-AUTH (SMTP AUTHentication) [RFC2554]: The protocol used for authentication when connecting to an SMTP server.

POP3 [RFC1939]: An email transfer protocol used when receiving email.

POP Before SMTP: An authentication mechanism using POP3 protocol, developed to guard against SPAM mail (email sent indiscriminately to a large number of destinations).

SASL (Simple Authentication and Security Layer) [RFC2222]: A framework that provides a common authentication processing mechanism for protocols that may require authentication, such as SMTP, POP3 and LDAP.

CRAM-MD5 [RFC2195]: A message digest functional algorithm that uses the MD5 algorithm to encrypt the challenge string and password.

DIGEST-MD5 [RFC2831]: A message digest functional algorithm developed as a countermeasure to dictionary and brute-force attacks. DIGEST-MD5 also supports realm designation (FQDN).

LDAP (Lightweight Directory Access Protocol) [RFC1777], [RFC2251]: A protocol used for accessing directory services that manage items such as user address books.

SMB (Server Message Block): A protocol used to enable file sharing between Windows PCs.
Note: The Ricoh MFP(s) to which this document applies support NTLM v1.

FTP (File Transfer Protocol): A protocol used when transferring files over a TCP/IP network.

15. FAX (MFP Models Only)

Overview of FAX operations

- The FAX function sends the scanned image data from the scanner engine to the other party's machine via a telecommunications line as a G3 or G4 FAX. Conversely, the MFP will only accept incoming FAX data that conforms to G3/G4 standards. The incoming document is then forwarded on to the printer engine for printing out.

- For Internet FAX transmission, the scanned image data is sent to the DCS, where it is converted into file attachment format for email transmission, after which it is sent to its destination via the network I/F. Conversely, the email FAX data received as an Internet FAX is converted into image data and then forwarded on to the printer engine for printing out.

- It is possible to store transmission files in the Document Server for sending at a later time. The file is saved to the HDD, after which commands can be issued from the operation panel or through the network to send the file to its destination. Conversely, incoming FAX data can be stored in the Document Server for printing out at a later time. The incoming FAX is saved to the HDD, after which commands can be issued from the operation panel or via the network to print out the file.

- With LAN FAX transmission, the image data received from the PC is then sent to its destination via a telecommunications line or network I/F.

- With all FAX transmission features, including Internet FAX, it is possible to restrict individual user access with the use of User Codes. For reception, it is possible to configure the MFP to receive only those transmissions accompanied by a predetermined code. Operational log entries are made for each transmission and reception job. This data is stored in non-volatile memory on the FCU, and can be viewed by printing out the Journal.

Data Flow

- After FAX transmission is initiated, the scanning command is sent to the ECS via the FCS, and the scanner engine is activated. At the same time, the data retrieval and transmission commands are sent to the FCU via the FCUH. The image data in memory is then sent from the scanning engine to the FCU, after which it is sent to its destination via the telecommunications line.

- With FAX reception, the incoming data is received by the FCU, which then sends the printing command to the FAX function via the FCUH and FCS. The FAX function then forwards the printing command to the ECS via the FCS, and the printing engine is activated. The FAX image data is then sent from the FCU to the printing engine for printing out.

- With Internet FAX transmission, the image data is sent from the FCU to the HDD and then on to the host I/F, which sends the data to its destination via the network. With Internet FAX reception, the image data is sent to the MFP over the network, after which it is sent to the FCU via the HDD and then stored in FCU memory. After this, the printing process is the same as described above.

- With Internet FAX transmission and regular FAX/IP-FAX memory transmission, the image data goes through MMR compression and is stored in SAF memory on the FCU. A battery for the SAF memory cell allows the data to be retained for one hour. The page location data is stored in SRAM, and can be erased from memory in SP mode by executing an SRAM initialization, SAF memory initialization or a factory settings reset.

- When sending a FAX that will also be stored to the Document Server, the image data is first stored in the HDD and then sent to its destination via the network or telecommunications line. Conversely, when receiving a FAX for storage to the Document Server, the image data is saved to the HDD.

- With LAN FAX transmission, the data sent from the PC is stored in the HDD or in the FCU if the MFP does not have an HDD. After this, the transmission flow is the same as described above.

- With IP-FAX transmission, the data flow is the same as with normal FAX transmission described above, except that instead of being sent via the telecommunications line, the image data is sent from the FCU to the FCS and then transmitted over the IP network via the network I/F of the controller. Similarly, IP-FAX reception does not receive incoming data through the telecommunications line, but rather through the network I/F of the controller. After this, the data is sent from the FCS to the FCU and then printed out.

- Incoming image data received through regular FAX reception, IP-FAX reception and Internet FAX reception is compressed and then stored in SAF memory. The data is then decompressed, after which the printing engine initiates the image printing process.

Data Security Considerations

- The FCU supports only G3 and G4 FAX protocols. Therefore, even if an initial connection is established with a terminal that does not use these protocols, the MFP will view this as a communication failure and terminate the connection. This prevents access via telecommunications lines and the FCU to internal networks, and ensures that no illegal data can be introduced via these lines.

- Internet FAX supports TIFF files and text-based email only, which is true for both reception and transmission. If the data received through this function is in any other format, a communication error will result.

- Internet FAX can also be set to forward incoming FAX data to specific destinations that have been preset in the MFP. With servers using SMTP reception/delivery, the receiver can set the server to prohibit the delivery of incoming Internet FAX documents from specific senders, restricting SMTP access.

- With LAN FAX transmission, the language processing subsystem is only able to process data that conforms to LAN FAX standards. If any other type of data is received, an error will result and the processing will be terminated.

- IP-FAX uses SIP for session initiation. SIP is a protocol that conforms to the H.323 and RFC326-1 standards prescribed by the ITU-T Recommendations. If any data is introduced which does not conform to these standards during transmission or reception, it will not be possible to establish SIP-based communication and the connection will then be terminated. Once a session is successfully established, communication is only performed in accordance with ITU-T recommended G3 FAX protocol. Since the MFP does not support any other type of communication protocol, if it attempts to connect to another machine that is not a FAX, it will not be possible to establish G3-based communication and the connection will then be terminated.

- Internet FAX operates under a SIP environment and undergoes a DIGEST authentication process, whereby the MFP's encrypted password must be registered with the SIP server and inside the MFP itself. When calling or registering with the SIP server, this server will initiate DIGEST authentication, after which the MFP sends the appropriate request message (encrypted password) to the server. Once the MFP is authenticated, the operator can send and receive Internet FAXes.

- When User Authentication is enabled, it is possible to set the authenticated user as the “Sender” of the FAX data. Similarly, for Internet FAX transmission, it is possible to set the authenticated user as the “Sender” of the email, i.e. the user who appears in the “From” field of the email.

- It is possible to restrict the use of the FAX function to specific users as well as to specific Document server documents, preventing any unauthorized access to this information.

- In order to guard against the reception of unnecessary or unwanted data, such as SPAM email, it is possible to register a list of authorized senders so that the MFP only accepts incoming data from these senders. Conversely, it is also possible to register a list of unauthorized senders, so that the MFP rejects any incoming data from these senders.

  For more details, please refer to Scanner (MFP Models Only).

Protection of the Journal and Documents in Document Server Storage

- When User Authentication is enabled, only authenticated users are permitted to perform any changes to the documents they transmitted, including deleting or canceling a transmission job or adding address (es). When the Journal is printed out, only the results for the authenticated user are shown on the printout.

- The only operation Machine Administrators are capable of performing on FAX jobs is job cancellation. They are not authorized to perform other operations such as adding or deleting destinations. Also, when the Machine Administrator prints out the Journal, the communication results for all users are printed out on the report.

Protection of FAX Transmission Operations

- By setting restrictions on address book destinations in addition to enabling User Authentication, it is possible to limit access to the destinations listed in the address book. After clearing authentication, general users are able to select only those destinations that have been set to allow this. In addition, the MFP can be set so that users can only transmit data to destinations registered in the MFP.

- It is possible to assign access restrictions to individual Document Server documents, so that only users with the required access privileges can perform operations on the document. Since this feature requires a specific access level to perform specific operations, it prevents unauthorized operations from being performed on the document (e.g. viewing, deleting). Also, documents that have not been assigned any access level cannot be sent as a FAX or printed out.

Protection of FAX Features Settings

- When Administrator Authentication or User Authentication is enabled, authentication is required in order to view or change any of the settings in Fax Features.

  Administrators can set the MFP so that general users are unable to make changes to the Fax Features settings, preventing any unauthorized alteration of these settings.

Extended Security Feature

- It is possible to set Extended Security to prohibit the transfer or forwarding of data, preventing any unauthorized sending of data to external destinations.

Note:

- The access control used for SMTP reception/delivery operates in accordance with RFC2305.
- The SMTP-AUTH feature operates in accordance with RFC2554.

- The Journal log (FAX job history log) is able to store up to 200 entries. When User Authentication is disabled, the Journal is automatically printed out every 50 jobs.

  When User Authentication is enabled, by default, the Journal is not automatically printed out. This is in order to prevent the private user information contained in the report from being accessible to all users. In this case, the oldest entry will be overwritten once the Journal reaches its 200-entry capacity. To ensure that this information is not lost, it is possible to have the entries sent by email to a specified destination, as well as to set the MFP to automatically print out the Journal even when User Authentication is enabled (overriding the default setting).

Job Log

- The FAX transmission results for each destination are sent to the LCS and then forwarded on to the HDD, where they are stored. For more details on job and access logs, please refer to Job/Access Logs.

16. NetFile (GWWS)

Overview of NetFile Operations

- NetFile operates via communication with the following applications installed on a network connected client PC:
  DeskTopBinder, Desk Top Editor For Production, SmartDeviceMonitor for Admin, ScanRouter, Web SmartDeviceMonitor for Admin.

Performing Operations on Document Server Documents (MFP models only)

- From DeskTopBinder or Desk Top Editor for Production, it is possible to print out Document Server documents that were stored using the Copier, FAX and Scanner functions or those that were edited and then returned to the MFP from one of the two DeskTop applications mentioned above. Commands issued from these applications allow documents stored using the FAX function to be sent as FAX data, and those stored using the Scanner function to be forwarded to ScanRouter. In addition, it is also possible to download Document Server files from the MFP to the PC, make changes to the bibliographic information of these documents or delete the documents themselves, all from within DeskTopBinder or Desk Top Editor for Production.

  Documents stored using each principal machine function can be protected with a password. Users are prompted for this password, even when attempting to perform the above operations from inside DeskTopBinder or Desk Top Editor For Production.

Restoring Files Back to the MFP (MFP models only)

- When Copier or Printer files that were originally sent from the MFP to Desk Top Editor for Production in TIFF or JPEG format are then restored to the MFP, the data is saved to the HDD as a separate file from the original one.

Viewing and Changing User Information Stored in the MFP/LP

- User data stored in the MFP/LP can be captured, added to, deleted, and changed from inside SmartDeviceMonitor for Admin; however this requires User Administrator access rights.

Viewing and Changing Machine Settings Stored in the MFP/LP

- Some machine settings stored in the MFP/LP can be viewed and changed from inside Web SmartDeviceMonitor for Admin. At present, it is possible to change a portion of the System Settings that can be changed from the MFP/LP operation panel; however these operations require authentication as a Machine Administrator, Network Administrator or User Administrator.

Transferring Job Log and Access Log Data to Web SmartDeviceMonitor for Admin

- The Netfile job log contains data related to job status (initiation, completion, any changes during the job), while the access log contains data related to operational events (authentication, operations performed on documents, administrator operations). Both logs are saved to the HDD by the LCS, and contain a date and time for each entry. As mentioned in section 1.9, it is possible to have the MFP/LP send the log data to Web SmartDeviceMonitor for Admin whenever any of the events described above occurs.
  Note: See "**Supplementary**" below for a list of the specific events for which Netfile job log entries are created.

- Only users who are registered with an administrator-level User Account in Web SmartDeviceMonitor for Admin can access the contents from a Web SmartDeviceMonitor for Admin client station.

Deleting Print Jobs

- From inside DeskTopBinder, it is possible to delete, pause, or resume any individual print job sent from the printer driver. From inside Web SmartDeviceMonitor for Admin, it is possible to delete all print jobs at once or the job in progress.

Data Flow

- Netfile supports two protocols for the sending and receiving of XML messages: Netfile Protocol and SOAP. With SOAP, once the PC client initiates the communication session, Netfile begins the appropriate processing operations in accordance with the specific request received.

Creating Thumbnails (MFP models only)

- The MFP creates thumbnail images in JPEG format for the first page of the image files stored in the HDD. The thumbnails themselves are also stored in the HDD as well. The specific operations performed by the MFP to create the thumbnails depend on whether or not the File Format Converter is installed.

- When the File Format Converter is not installed:
  - When the image data is saved to the HDD, the MCS uses its modules to create a thumbnail of the first page of the image data.
  - When the File Format Converted is installed:
    When the image data is saved to the HDD, the IMH uses its modules to create a thumbnail of the first page of the image data. The first page is read into memory, after which the File Format Converter compresses it and converts it into image data. The MFP software then creates the thumbnail from this data. If a request is received for thumbnails for page 2 or onward, Netfile sends the request to the IMH via the MCS. The IMH then generates the thumbnail for the requested page(s) in the same way as described above for page 1.

Viewing Thumbnails (MFP models only)

- Netfile loads the requested thumbnail data directly from its storage location on the HDD, and then sends it to the PC via the NCS.

Deleting Thumbnails (MFP models only)

- When the number of thumbnails for pages 2 and onward created at the request of Desk Top Editor for Production reaches a certain limit, Netfile will choose the oldest thumbnail and send a request to the MCS to delete it. The MCS then deletes the specified thumbnail from HDD memory. Also, the MCS deletes all thumbnails for pages 2 and onward from HDD memory whenever the main power is turned on or a system reset is performed.

Downloading Document Server Files to the PC (MFP models only)

- From DeskTopBinder or Desk Top Editor for Production, it is possible to download full images stored on the MFP HDD. Netfile loads the requested image data stored in the HDD via the MCS, and then sends it to the PC via the NCS. Since documents created using the Copier and Printer functions are saved to the HDD in a Ricoh-original data format, the File Format Converter is necessary to convert the data into a commonly used data format (JPEG, JPEG2000, TIFF or PDF). To do this, the IMH uses its own internal modules in tandem with the File Format Converter. For models that have a DESS module, it is possible to download images as encrypted PDF data.

  Note: A similar data flow is used when Document Server files or Copier/Document Server print backup files are captured.

Printing out Document Server Documents (MFP models only)

- When printing out documents stored in the MFP from DeskTopBinder or Desk Top Editor For Production, Netfile sends the printing command to the ECS. Working in tandem with the IMH, the ECS then loads the specified document out of HDD memory and sends it along to the printing engine for printing out.

Transmitting FAX Document Server Files (MFP models only)

- When the MFP receives instructions from DeskTopBinder or Desk Top Editor for Production to transmit a file that was stored to the HDD using the FAX function, Netfile sends the FAX transmission command for the specified file to the FCS. Working in tandem with the IMH, the FCS then loads the specified document out of HDD memory and sends it along to the FCU for FAX transmission.

Downloading FAX Reception Documents to the PC (MFP models only)

- Netfile loads the image data out of HDD memory via the MCS, after which the data is sent to the PC via the NCS.

Forwarding Stored Scanner Documents (MFP models only)

- When the MFP receives instructions from DeskTopBinder or Desk Top Editor for Production to forward a Scanner document, Netfile sends a forwarding command for the specified file to the DCS. Working in tandem with the MCS and IMH, the DCS then loads the specified document out of HDD memory and sends it along to the PC. The transmission protocols used are FTP, HTTP and HTTPS.

Forwarding Image Data with Capture

- With the Capture feature, the primary machine function temporarily stores the image data to the HDD in tandem with the MCS and IMH. A request is then made to the GWWS via the SCS to capture the image. In tandem with the MCS and IMH, the GWWS in turn loads the image data out of HDD storage, converts the image to a file type for Capturing. If the file was created using the Copier or Printer function, the GWWS requests the IMH (via the MCS) to convert the file into a commonly-used format using the File Format Converter. Finally, the GWWS temporarily stores the new file in the HDD.

- Following this, the GWWS requests the DCS to forward the new file it just saved to the HDD. The DCS in turn loads the file out of HDD memory and forwards it to ScanRouter. Three transfer protocols are available for sending captured documents to ScanRouter: FTP, HTTP and HTTPS.

- For details on the data flow that is followed when images created with each primary machine function are stored to the HDD, please refer to the “Data Flow” explanations in each section of this document.

Restoring Images Back to the MFP (MFP models only)

- When Copier or Printer files which were originally downloaded from the MFP to Desk Top Editor for Production in TIFF or JPEG format are then restored to the MFP, the GWWS sends the data to the NCS, which then sends it to the HDD for storage via the MCS. This pathway is the reverse of that used to send stored images to the PC. Before storage, the IMH uses its modules and the File Format Converter to convert the file format from TIFF/JPEG2000 to a Ricoh-original format. These “restored” files are actually separate files than their originals, and are stored in the HDD in a separate location.

Viewing and Changing User Data Settings Stored in the MFP/LP

- From SmartDeviceMonitor for Admin, it is possible to view and change the user data settings stored in the MFP/LP. Only users authenticated as User Administrators are able to change these settings. User data is stored in the HDD and is managed by the UCS.

- When the MFP/LP receives a request to view this data, the UCS loads the data out of HDD memory, after which Netfile obtains the information via communication with the UCS and related modules. Netfile then sends the data to SmartDeviceMonitor for Admin via the network. When the MFP/LP receives a request to make changes to some of the data, Netfile obtains the new settings from SmartDeviceMonitor for Admin, after which it communicates with the UCS and related modules. The UCS then saves the new data to the HDD. In cases where data is received from SmartDeviceMonitor for Admin for an address book data backup or restore, the data is encrypted before it is sent. For more details on the UCS internal management of the address book data, please see Data Protection.

- Even in cases in which SSL is not used, GWWS encrypts the user's password using the DESS module (but does not encrypt any other part of the user data). The DESS module also communicates directly with the UCS to encrypt the Address Book data when performing an Address Book backup.

Viewing and Changing Machine Configuration Data Stored in the MFP/LP

- In order to view or change the machine configuration settings obtained by Web SmartDeviceMonitor for Admin, users must have an administrator-level User Account registered in this utility. The machine configuration data is managed by multiple modules, including the FCS, NCS, DCS and SCS. The main storage location of the data is the NV-RAM. When a request is received to view configuration data, these modules directly assess the NV-RAM. Netfile then communicates with these modules to load the data out of memory and send it on to Web SmartDeviceMonitor for Admin.

- When making changes to the current MFP/LP settings, Netfile receives the new settings from Web SmartDeviceMonitor for Admin and forwards them on to the appropriate module(s). The settings are then saved to the NV-RAM.

Transferring the Job Log and Access Log Data

- To send log data from the MFP/LP to Web SmartDeviceMonitor for Admin, GWWS communicates with the LCS, which uses its internal modules to load the necessary information out of HDD memory. GWWS then encrypts the data using the DESS module and sends it as a Web SmartDeviceMonitor for Admin client over an SSL connection.

  Note: For an overview of the contents and operations of the Netfile job/access logs, please refer to Job/Access Logs and "**Transferring Job Log and Access Log Data to Web SmartDeviceMonitor for Admin**" above.

Deleting, Pausing, and Resuming Print Jobs

- The operator can delete, pause, or resume a print job from DeskTopBinder. To do this, DeskTopBinder sends Netfile the request along with a specific track ID, which it manages internally for each job. Netfile in turn forwards this on to the Printer function.

- When deleting a print job from Web SmartDeviceMonitor for Admin, only the request is sent. A track ID is unnecessary in this case, as the operator may only select the job in progress or all jobs for deletion.

Supplementary:

- **Passwords for Stored Documents (MFP models only)**

No operations can be performed on password-protected stored documents unless the correct password is entered, even when attempting to do so from DeskTopBinder or Desk Top Editor For Production on a network-connected PC. During the bi-directional communication between these applications and the MFP, data is exchanged in HTTP text or XML text format. Information such as passwords and User Codes are included in this text data, and are encrypted before being sent.

- **Events Which Trigger Netfile Job Log Entries (MFP models only)**

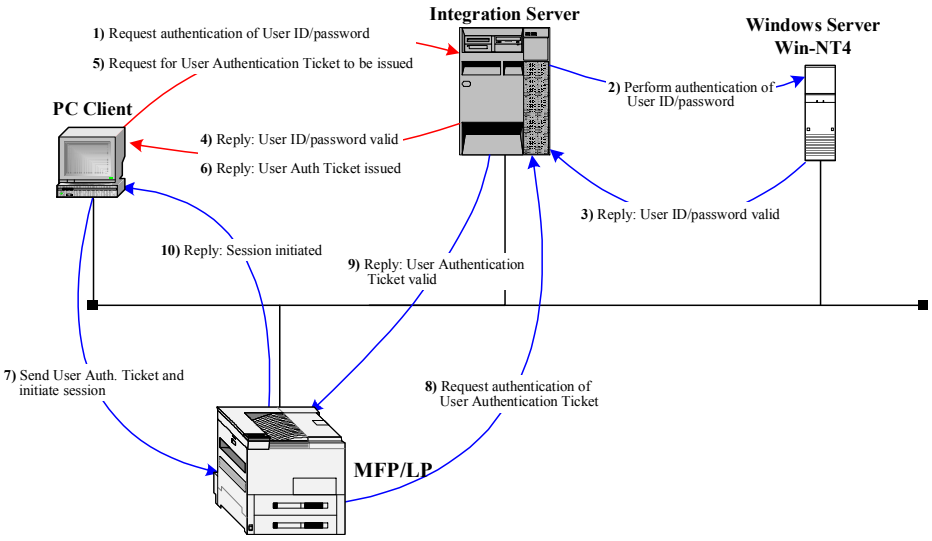
Entries are created in the Netfile Job Log whenever any of the following events occur:

- A print job is initiated from DeskTopBinder on a Document Server file
- A transmission job is initiated from DeskTopBinder on a FAX Document Server file
- A sending/forwarding job is initiated from DeskTopBinder on a Scanner Document Server file
- A download is initiated from DeskTopBinder on a FAX Document Server (Reception) file
- A download is initiated from DeskTopBinder on a Scanner Document Server file
- A captured Document Server file is restored to the MFP from Desk Top Editor For Production

➢ **User Authentication Tickets (MFP models only)**

When using User Authentication to connect to the MFP from a PC client station, the user must be authenticated using the User ID and password information sent to the MFP. However with the use of pre-issued User Authentication Tickets, users can access the MFP without having to input the necessary authentication information each time a session is initiated.

First, to be issued a User Authentication Ticket, the user connects to the Integration Server from a PC client station, at which time authentication is performed using the User ID and password. Once the server authenticates the user, the ticket is sent to the MFP. When user then accesses the MFP, e.g. to download stored images or perform other operations, the ticket is sent from the PC client to the MFP along with the request to initiate a new session. The MFP then communicates with the Integration Server to verify the identity of the user.


Integration Server
Windows Server
Win-NT4
1) Request authentication of User ID/password
5) Request for User Authentication Ticket to be issued
2) Perform authentication of User ID/password
PC Client
4) Reply: User ID/password valid
6) Reply: User Auth Ticket issued
3) Reply: User ID/password valid
10) Reply: Session initiated
9) Reply: User Authentication Ticket valid
7) Send User Auth. Ticket and initiate session
8) Request authentication of User Authentication Ticket
MFP/LP

Network Topology for a System Using Integration Server Authentication (Sample)

17. Data Security Considerations

SOAP Communication Sessions

- SOAP communication supports SSL (Secure Sockets Layer), ensuring the proper security during communication sessions. Even in cases where SSL is not used, the client (PC) identifies the server (MFP/LP) via a unique session ID. Only after the MFP/LP identifies the client through this session ID will it accept any requests from the client. This session ID is a randomly generated value, making it extremely difficult for third parties to surmise its contents and use it to impersonate the client. The session time limit of 30 seconds provides additional security against this type of threat.

- To increase the level of security even further, it is possible to use usernames and passwords stored in the MFP/LP to authenticate clients, so that any clients who do not know this information will be unable to perform remote Netfile operations. As mentioned above, this password is encrypted before being sent over the network, preventing third parties from accessing or altering any information stored in the MFP/LP.

Usage of Documents Stored in the MFP (MFP models only)

- The protections provided for documents stored in the MFP are the same, regardless of the access method (over the network versus from the MFP operation panel). The ACL operates in accordance with the settings in the MFP.
  Note: Please refer to Protection of Document Server Documents for more details.

- For password-protected documents, it is not possible to perform any operations on the file unless the correct password is entered. As described above (“Protection of Passwords for Stored Documents”), communication between the MFP and DeskTopBinder or Desk Top Editor For Production is performed using text written in HTTP and XML format, for both sending and receiving. The password is embedded in this text data when it is sent to the MFP. Since User Codes and passwords are encrypted before being sent, the information itself would be indecipherable even if it were intercepted along the communication path.

- For each individual user, it is possible to restrict the use of specific functions of DeskTopBinder and Desk Top Editor for Production. To use any of these functions, however, users need to be pre-registered in the MFP.

- User access control can also be performed for FAX reception documents stored in the MFP. Operations on these documents can only be performed by users already registered in the FAX function as individual users or as part of a group.

Restoring Files Back to the MFP (MFP models only)

- Netfile will reject any data it receives that does not conform to preset formats, regarding it as illegal data. If the operator attempts to restore image data from Desk Top Editor For Production to the MFP, and the data does not conform to the standard format, the File Format Converter will not be able to convert the file and the data will be destroyed without any adverse effect on data stored in the MFP. It is therefore not possible to introduce illegal data when restoring data to the MFP.
  Note: Since Netfile treats the data it receives through this process as a separate file from the one originally sent to the PC, the destruction of such illegal data does not affect the original file.

Viewing and Changing User Information Stored in the MFP/LP

- As mentioned above, user data stored in the MFP/LP can be captured, added to, deleted, and changed from inside SmartDeviceMonitor for Admin; however this requires User Administrator access rights (see Data Protection for more details).

Viewing and Changing Machine Settings Stored in the MFP/LP

- As mentioned above, in order to view or change the machine configuration settings obtained by Web SmartDeviceMonitor for Admin, users must have an administrator-level User Account registered in this utility. Similarly, the network settings can only be changed by users logged in as Network Administrators, and the user settings can only be changed by those logged in as User Administrators. The access control settings for an individual user can only be viewed by the user who is registered with that account, or by any of the administrators mentioned above. These administrators are the only individuals who can view the user counter values.

Sending the Log Information to Web SmartDeviceMonitor for Admin

- Please refer to Job/Access Logs.

User Authentication Tickets (MFP models only)

- User Authentication Tickets provide increased security by making it possible to perform operations on multiple MFP devices from the same PC without having to send the user's password over the network each time.

Deleting, Pausing or Resuming Print Jobs

- To delete the current job or all active jobs at once, the operator must have Machine Administrator-level access privileges. In addition, the operator must have already logged in to SmartDeviceMonitor for Admin as a Machine Administrator.

- As mentioned above, the operator can delete, pause, or resume a print job from DeskTopBinder. The printer driver uses a track ID to identify each individual print job. When the operator initates the deletion, pause, or resumption of a print job, DeskTopBinder sends Netfile the request along with the track ID for the job in question. As long as the track ID is not stolen from the communication path between the PC and MFP/LP (which can be prevented by enabling SSL encryption), or from the PC itself, it is impossible to perform any operations on these print jobs. Even if the track ID were stolen somehow, the result would be limited to the deletion, pausing, or resumption of the print jobs in question. There would be no threat of access to the files themselves.

18. Web Applications

Web Server Framework

The MFP/LP Web Server was developed exclusively by Ricoh, Co. Ltd.

Encrypted Communication Support

- The Web server installed on the MFP/LP supports SSL communication. Since the MFP/LP is accessed via an HTTPS connection, all input/output data is encrypted (incl. authentication ID, password, and cookie). This allows for safe and secure communication between WebImageMonitor and the MFP/LP. It is possible to set the MFP/LP so that it will reject HTTP-based communication, which does not encrypt the data mentioned above, such that it will only accept HTTPS-based communication.

User Authentication Support

- WebImageMonitor supports the access control functions described above in “Authenticaion/Access Control”. These functions provide greater security by prohibiting unauthenticated users from changing any settings as well as limiting the number of items that can be viewed.

Protection Against Cross-site Scripting (XSS)

- “Cross-site scripting” is a security threat that refers to the introduction of malicious script into the data stored on a Web server with the purpose of causing the following damage when a valid user accesses a Web page associated with that server.
  - ✧ User information is accessed, such as data stored in cookies
  - ✧ Files stored on the PC are accessed or destroyed
  - ✧ URL redirection to malicious Web sites

- As mentioned above, authentication is required before any changes to the MFP/LP settings can be made from WebImageMonitor. This ensures that users without valid accounts are not able to introduce script containing malicious data.

- The MFP/LP sanitizes all HTML data that is sent from an MFP/LP Web application to WebImageMonitor. One of the strongest known countermeasures against cross-site scripting, data sanitizing deletes or neutralizes selected character strings designed to function as HTML tags or script.

Protection Against URL Buffer Overflows

- URL buffer overflow attacks occur when intentionally oversized URL strings are sent to a Web server with the intent of overflowing the buffer's storage capacity, causing the server to shut down. WebImageMonitor prevents such trouble by limiting the length of the URL strings it will accept, rejecting any requests that exceed this limit.

- In addition, authentication is performed before any settings can be changed, ensuring that malicious data cannot be introduced via illegal access.

Protection Against Session Hijacks

- A "session hijack" refers to when the session ID stored in a cookie is obtained in order to illegally access or otherwise use a session for malicious purposes.

- WebImageMonitor employs the following countermeasures to minimize the threat of session hijacks:
  - The session ID is randomized, which makes it very difficult for third parties to surmise its value
  - Communication is protected by SSL, preventing theft of any data or messages exchanged
  - The above-mentioned countermeasures for cross-site scripting prevent cookies from being illegally accessed

- In addition, there are also security measures to minimize any potential threat to the MFP/LP in the unlikely event the session ID were somehow stolen:
  - The session ID is given an expiration date
  - The session ID contains no information whatsoever that could be linked to individual user data stored in the MFP/LP

Protection Against the Setting of Illegal URLs

- The optional URL setting in WebImageMonitor can only be changed by users authenticated as Network Administrators.

19. WebDocBox (MFP models only)

Overview of WebDocBox Operations

- WebDocBox allows users to issue commands via a Web browser to view, capture, print, send (email, FAX, forward) and delete Document Sever image files that were saved to the MFP HDD using the Copier, Printer, Scanner and FAX functions, as well as those that were restored to the MFP using Desk Top Editor For Production. It is also possible to view thumbnails of these images.

Data Flow

- WebDocBox supports HTTP, a protocol used by Web browsers installed on network-connected computers. The session is initiated when the first request for connection is received from the Web browser, after which WebDocBox sends commands to the shared service layers in accordance with the specific operations requested. If 30 minutes passes with no additional access attempts from the same browser, the session is terminated. To initiate a new session, it is then necessary to access the WebDocBox top page, i.e. the main screen that displays the list of Document Server files.

Viewing Thumbnails of Stored Image Data

- The MCS creates thumbnails of the Document Server image files that were stored in the HDD using each machine principal function, after which the thumbnails are stored in the HDD. When the MFP receives a request from the Web browser to view a thumbnail, WebDocBox instructs the GWWS to send the requested thumbnail to the PC. GWWS loads the thumbnail directly from HDD memory and then sends it to the PC via the NCS.

Viewing and Changing the Properties of Stored Image Data

- By sending a request from the Web browser to view the properties of stored image data, it is possible to view information such as the date/time at which the file was stored and the size of the original for the first page. By sending a request to change the property settings, it is possible to change such items as the filename, document name and password. These operations are carried out by the GWWS and MCS, after which the requested information or results of the requested operation are sent to the PC via the NCS.

Sending Stored Image Data to the PC

- When the MFP receives a request from the Web browser to send stored image data to the PC, WebDocBox instructs the GWWS to send the requested data. GWWS loads the requested data from HDD memory via the MCS and then sends it to the PC via the NCS. Since Copier and Printer documents are saved to the HDD in Ricoh-original file format, it is necessary to use the File Format Converter to convert the data to JPEG or TIFF format.

Printing Out Stored Image Data

- When the MFP receives a request from the Web browser to print out stored image data, WebDocBox instructs the ECS to print out the requested data. The ECS, in tandem with the IMH, loads the requested data from HDD memory and sends it to the printing engine for printing out.

Sending Stored Image Data

- When the MFP receives a request from the Web browser to email, forward or FAX image data stored in the MFP HDD, WebDocBox instructs either the DCS or FCS to carry out the operation. The DCS or FCS, in tandem with the IMH, loads the requested data from HDD memory and transmits it via the NCS or FCU.

Data Security Considerations

- As a security feature common to all Web applications, it is possible to perform access control by allowing connection only with users who provide a specific IP address when the session is initiated. Users who do not provide an authorized IP address are not even able to view Document Server data. In addition, it is possible to prevent the viewing and altering of data through the use of encrypted communication (HTTPS over SSL).

- With the use of User Authentication, it is possible to limit the conditions under which remote operations can be performed on Document Server files. Only users who have been pre-approved for access and clear the authentication process are allowed to perform the remote operations. Additionally, it is possible to place limits on the specific operations that each registered user is capable of performing. Users are unable to perform operations that have been prohibited, even if they clear the authentication process. This prevents any potential leakage or alteration of image data.

- It is possible to protect individual Document Server documents with a password (see Document Server Documents (MFP models only) for more details).

- It is possible to restrict remote access to stored documents using the same ACL mentioned in section 1.52. Users logged in as Document Administrators are able to disable the password lock as well as view, edit and delete all documents. However, Document Administrators are not able to send (FAX, email, forward), capture or print out the documents.

- When sending stored image files to the PC in PDF format, it is possible to encrypt the file as well as set a password for decrypting the PDF data at the PC side. This prevents any illegal use of the data in the unlikely event the transmission is intercepted.

Job Log Data

- An entry is added to the job log for each individual job, containing information on the job settings (e.g. simplex or duplex, paper size), completion status (whether completed successfully or not) and user identification (in cases where User Authentication was enabled). The information is sent to the HDD via the LCS. For more details on job and access logs, please refer to Job/Access Logs.

20. Optional Features

@Remote

Overview of @Remote Operations

- "@Remote" refers to a remote machine management service that manages and monitors the MFP/LP status from a remote location called the @Remote Center. Information and commands are exchanged directly between the MFP/LP and @Remote Center, or between these two points via an intermediary device called RC Gate, which is connected to the MFP/LP in the same LAN.

- When communicating as a "client", the MFP/LP continually monitors its own status and informs RC Gate or @Remote Center when action is required, such as when parts have reached their periodic replacement limit or an abnormal machine condition is detected. When communicating as a "server", the MFP/LP receives requests from RC Gate or @Remote Center for status information such as the amount of toner remaining in the MFP, after which it provides this information to whichever device has requested it.

- @Remote communication to and from the MFP/LP is only possible when the relevant SP mode switch has been turned ON. It is therefore possible to prohibit communication with RC Gate or @Remote Center by turning this switch OFF.

Data Flow

- The communication protocol used is different depending on whether the MFP/LP is communicating with the @Remote center directly, or via the RC Gate. The NRS module controls all primary @Remote functions inside the MFP/LP.

Communicating with the @Remote Center via RC Gate

When the MFP/LP communicates with RC Gate as a client (e.g. notifying the center of a malfunction)

When the SCS detects an abnormal condition in the MFP/LP or other status-related notification, it will notify the NRS module. After this, the NRS module obtains more detailed information via the SCS and then converts it into a special format for transmission to the @Remote Center. Finally, the data is sent to RC Gate via the NCS module, and then on to the @Remote Center.

The NCS module communicates with RC Gate via the host I/F over an SSL connection. The authentication process uses the information on the relevant digital certificates to verify the identity of both machines. To do this, the NRS module uses the DESS module and checks the information contained in the digital certificates. If both machines judge that the other is the legitimate server/client, SSL encrypted communication is established, whereby the MFP/LP sends the relevant information to RC Gate in an encrypted state via the host I/F.

When the MFP/LP communicates with RC Gate as a server (e.g. taking a counter reading)

Requests for information sent by RC Gate to the MFP/LP are received by the host I/F and then forwarded to the NCS module. Before establishing the communication session, the NCS module initiates a two-way authentication process whereby the contents of both machines' digital certificates are verified. To do this, the NRS module uses the DESS module and checks the information contained in the digital certificates. As described above, if both machines judge that the other is the legitimate server/client, SSL encrypted communication is established. The MFP/LP receives the information request from RC Gate, after which the information is decrypted by the NCS module and then sent along to the NRS module. The NRS module retrieves the required information from the SCS module, converts the data into @Remote-transmission format, and then forwards the data to the NCS module. The NCS module encrypts the data for SSL transmission and sends it to RC Gate.

Communicating with the @Remote Center Directly (via the Internet)

Functionally, the server/client relationship between the MFP/LP and @remote center is two-way, as described below. However in terms of actual data flow, the MFP/LP is always an https client of the @remote center.

When the MFP/LP communicates with the @Remote Center as a client (e.g. notifying the center of a malfunction)

When the SCS detects an abnormal condition in the MFP/LP or other status-related notification, it will notify the NRS module. After this, the NRS module obtains more detailed information via the SCS and then converts it into a special format for transmission to the @Remote Center. Finally, the data is SSL-encrypted and sent to the @Remote Center via the NCS module.

The NCS module communicates with the @Remote Center via the host I/F over an SSL connection. Both the MFP/LP and @Remote center perform a bi-directional, digital certificate-based SSL authentication process to verify that the other is a valid @Remote communication terminal, after which the NRS module accesses the DESS module and compares the @Remote Center ID information sent from the center with the ID information already stored in the MFP/LP. (As the @Remote Center ID is unique, each MFP/LP is only able to connect to one @Remote Center). If both judge that the other is the legitimate communication terminal, SSL encrypted communication is established, whereby the MFP/LP sends the relevant information to the @Remote Center in an encrypted state via the host I/F.

When the MFP/LP communicates with the @Remote Center as a server (e.g. taking a counter reading)

In order to enable the MFP/LP to poll the @Remote Center, the NRS module sends the necessary polling information to the NCS module. The NCS module then communicates with the @Remote Center via the host I/F over an SSL connection. The authentication process is the same as described in the paragraph above.

Requests from the @Remote Center sent as polling responses are received by the NRS module. After this, the NRS module obtains more detailed information via the SCS and then converts it into a special format for transmission to the @Remote Center. Finally, the data is SSL-encrypted and then sent to the @Remote Center via the NCS module.

Data Security Considerations

- As mentioned above, communication between the MFP/LP and RC Gate is conducted on an SSL-encrypted communication path. Since digital certificate-based authentication takes place before any data exchange is performed, this ensures that RC Gate is the only remote device to which the MFP/LP can be connected.

- The MFP/LP's digital certificate for the @Remote function is embedded in the MFP/LP during the last stage of factory assembly.

- With the use of SSL communication, symmetric key cryptography ensures that the data being transferred cannot be leaked to third parties. Security is increased even further by the fact that the symmetric key used is not a static key, but rather one that is generated every time a new session is initiated.

- The internal layout of the modules is such that the NRS module must always exchange machine information with RC Gate via the SCS module. Although it is possible for RC Gate to obtain specific machine information stored in the MFP/LP, there is no route possible that would allow access to the image data. It is therefore not possible for any image data stored in the MFP/LP to be mistakenly sent to the @Remote Center.

21. CSS (Customer Support System) – MFP Models Only

Overview of CSS Operations

- The CSS control center sends a request for service-related information to the MFP across a telecommunications line, which is then received by the LADP (line adapter telephony box). The LADP then obtains the requested information via the CSS I/F and sends it back to the CSS control center. The service-related information requested by the CSS control center includes data related to external charge devices (e.g. serial number, counter values), as well as other data.

- If an abnormal condition is detected in the MFP, the MFP sends a command to the LADP via the CSS I/F to inform the CSS control center of the condition. The LADP then contacts the CSS control center via a telecommunications line and reports the information.

Data Flow

- The SCS module extracts the information requested by the LADP out of the pre-defined RAM location, and then sends it to the LADP via the CSS I/F. When an abnormal condition is detected in the MFP, the SCS module reports this information to the LADP via the CSS I/F.

Data Security Considerations

- For MFP products that support the CSS function, a single-chip microcontroller is used to control all CSS-related communication, including protocol conversion and the destruction of any illegal data. On the structural layout diagram, this chip is located at the CSS I/F. The actions that the MFP CPU can perform are limited to three types of pre-defined commands: Read, Write and Execute. These are the only commands that can pass through the CSS I/F, i.e. the only actions that the external source (CSS control center) can instruct the MFP CPU to perform. Through these commands, the MFP performs the same processing tasks as when receiving the commands from the operation panel, making it impossible for the operator to execute external programs or freely read/write to a memory area of their choosing.

- Through this filtering, the CSS I/F will destroy any command other than the three pre-defined commands mentioned above. In addition, the firmware for the single-chip microcontroller is stored in a Mask ROM, making it impossible for its contents to be overwritten.

22. Copy Data Security Feature

Overview of Copy Data Security Operations

- The Copy Data Security feature acts to discourage unauthorized copying of confidential documents. There are two aspects to the feature:
  - Marking the copy/print with a visible, embedded pattern
    Note: The marking aspect is a standard feature on MFP/LP models.
  - Detecting the pattern if a copy is attempted, and then graying out the entire image
    Note: The detection aspect is provided as an optional feature on MFP models only (Copy Data Security Unit).

Marking:

- If the user selects the Copy Data Security feature when making the first copy of a document or printing out the document for the first time from the printer driver, a pre-defined pattern will be embedded in the background area of the resulting image to demarcate that copying of the image is prohibited. Users can select from among several patterns, as well as add a text string such as "Copying of this document is prohibited" or the date, time or name of the user who created the original document (details below).
  Note: Documents for which the Copy Data Security feature has been selected cannot be saved to the Document Server.

Detection/Graying:

- If a user then attempts to make a copy of an image containing the embedded pattern (or store the image to the MFP Document Server), and the optional Copy Data Security Unit is installed on that MFP, the pattern will be detected and a buzzer will sound. The image is then grayed-out to hide the original contents and then exited to the tray. In addition, a log entry of the event will be added to the Access Log, along with the date, time and username.
  If a user attempts to make a copy of an image containing the embedded pattern on an MFP without the optional Copy Data Security Unit, including products of another make, the resulting image will not be grayed out. However, it will be much more indecipherable due to the superimposition of the pattern on the original image. In addition, if the user entered a text string to be embedded into the pattern when printing out the original document, the text will be made visible when a copy of the document is made. This optional text field can be set to a number of different character strings to suit the operator's needs, such as "Copying of this document is prohibited", the date on which the document was created, or the name of the user who created the document. By making this information visible, it is possible to further deter the unauthorized copying of documents.

Note: The exact appearance of the optional text string (size, image density, etc.) will depend on the type and condition of the machine making the copy.

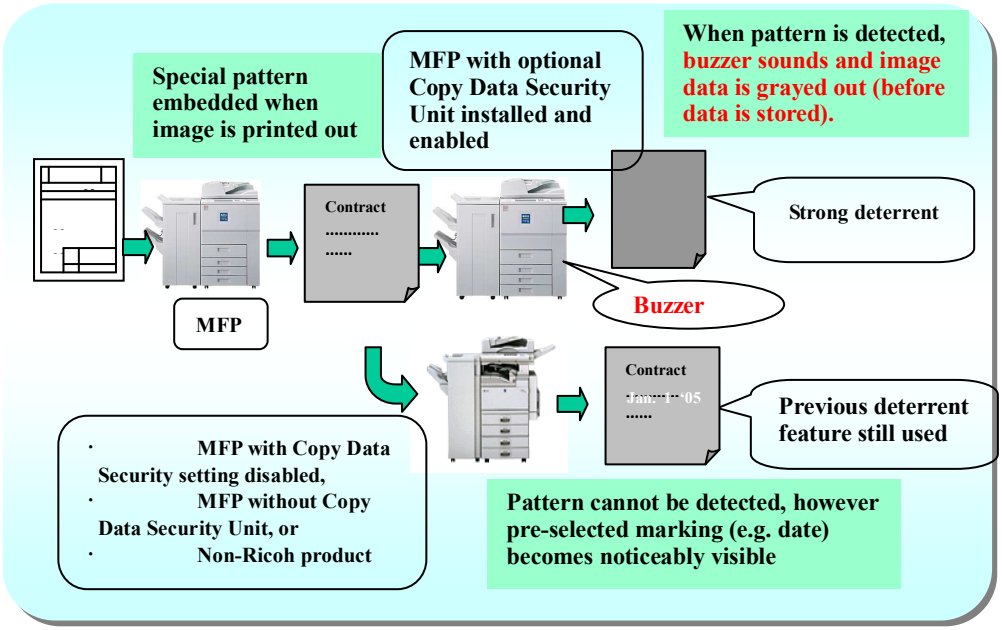
Data Flow

Marking:

- The data flow for when the Copy Data Security feature is selected at the time a print job is performed is virtually the same as that of regular print jobs (see Printer). The printer language-encoded data sent from the host computer is interpreted by the language processing subsystem, after which it is converted into image data. It is then combined with the background pattern selected by the user and stored temporarily in the Page Memory in binary bitmap format.

Detection/Graying:

- The optional Copy Data Security Unit, which is necessary in order to detect the embedded pattern on the paper, functions as part of the image processing performed during the scanning phase, i.e. before the image data is temporarily saved to memory. As the scanning engine scans the image, the Copy Data Security Unit examines the scanned data for the presence of an embedded pattern. Once the unit detects the presence of the pattern, demarcating the data as a confidential document, the buzzer is sounded and the scanned data is grayed out from that point onward. Following this, an entry for the event itself is stored in the Access Log, along with the username.


Special pattern embedded when image is printed out
MFP with optional Copy Data Security Unit installed and enabled
When pattern is detected, buzzer sounds and image data is grayed out (before data is stored).
Contract
Strong deterrent
Buzzer
MFP
Contract
Previous deterrent feature still used
· MFP with Copy Data Security setting disabled,
· MFP without Copy Data Security Unit, or
· Non-Ricoh product
Pattern cannot be detected, however pre-selected marking (e.g. date) becomes noticeably visible

Other Conditions of Use

On some MFP models, one or more of the following limitations exist:

- The Copy Data Security Unit and FAX option cannot be installed on the same MFP.
- The Copy Data Security Unit and FAX option can be installed on the same MFP, but the detection/graying process described above does not work when sending a FAX.

- When the Copy Data Security Unit is installed:
  - The Scanner function cannot be used.
  - Magnification ratios for Copier and Document Server documents are limited to 50% or greater.

Note: To restore usage of the Scanner function and all magnification ratios for Copier and Document Server documents, it is necessary for a service technician to remove the Copy Data Security Unit and the Administrator to disable the function's setting.

23. Device SDK Applications (DSDK)

Overview of Operations

- DSDK applications developed by Vendors are able to make use of the scanning, printing and other functions of the MFP/LP by calling the VAS (Virtual Application Service), which wraps the GW-API for the standard principal functions of the MFP/LP. This arrangement allows SDK applications to run as additional principal functions themselves once installed.

- There are two types of DSDK applications that are able to run on the MFP/LP: Type 1 and Type 2. Type 1 applications are written in the C programming language, and are usually developed for use with productivity-oriented principal machine functions. Type 2 applications are Java-based, and are composed of main program files (JAR files) which run on top of a CVM (Compact Virtual Machine) Java core developed by Sun Microsystems. The GW system regards the CVM Java core itself as a single Type 1 SDK application.

Note: CVM ver1.1/J2SE1.4 (or equivalent) is required for wide-format MFP models, and CVM ver1.01/J2SE1.3 (or equivalent) for all other models.

- Type 2 applications initiate MFP/LP scanning and printing operations by calling an extended class (called an MFP class), which then uses the JNI (Java Native Interface) to call the VAS directly or libraries provided by a Type 1 application.

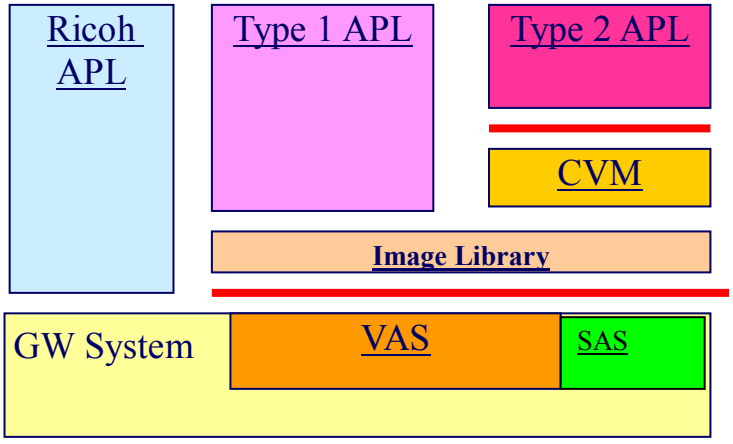


Fig. 1

Installation

- DSDK applications are installed via Type 1 or Type 2 SD cards into partitions and directories in the MFP/LP HDD or SD card itself that are specifically allocated for DSDK applications.

- The SAS (SDK Application Service) in the MPF contains an installer for DSDK applications. When the main power is turned ON, the SDK installer inside the SAS checks the pre-defined area in the SD card for the necessary installation files and then performs the installation. For more details on the authentication process performed at installation, see Authentication of SDK Applications at Installation below.

- **(MFP models only):** Type 2 applications can be further divided into Xlet applications and Servelet applications. Xlet applications have the capability of displaying their own screens on the MFP/LP operation panel, whereas Servelet applications do not.

- **(MFP models only):** A maximum of three Type 1 applications can be installed on the MFP/LP at one time, depending on the amount of virtual memory (VM) that the applications require. As mentioned above, the GW system regards the CVM Java core itself as a single Type 1 application. Therefore if one Xlet and one Servelet application are installed at the same time, the MFP/LP will allow one additional Type 1 application to be installed (see Fig. 2 below).

- **(MFP models only):** A maximum of twenty applications can be installed on the MFP/LP at any one time (total combination of Xlet and Servelet applications), depending on the total amount of VM that the applications require.

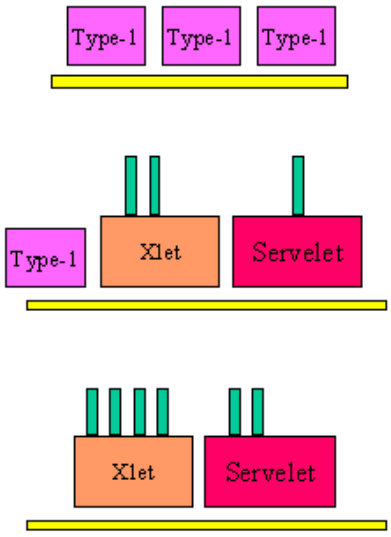


Fig. 2: Three Examples of Simultaneous Installation of Type 1 and 2 Applications

Overview of SDK Application Functions

- As mentioned above, Vendors can create their own DSDK applications for installation on the MFP/LP. Vendors are provided with an image library, which simplifies complex internal MFP/LP operational flows into concise, predefined methods for simple execution. This allows Vendors to develop their applications relatively easily.

  Examples of such methods include:

  - Scanning the original according to specified conditions, and then storing the image on the HDD **(MFP models only)**.
  - Searching for an image file stored on the MFP/LP HDD, and then retrieving or printing out the file.

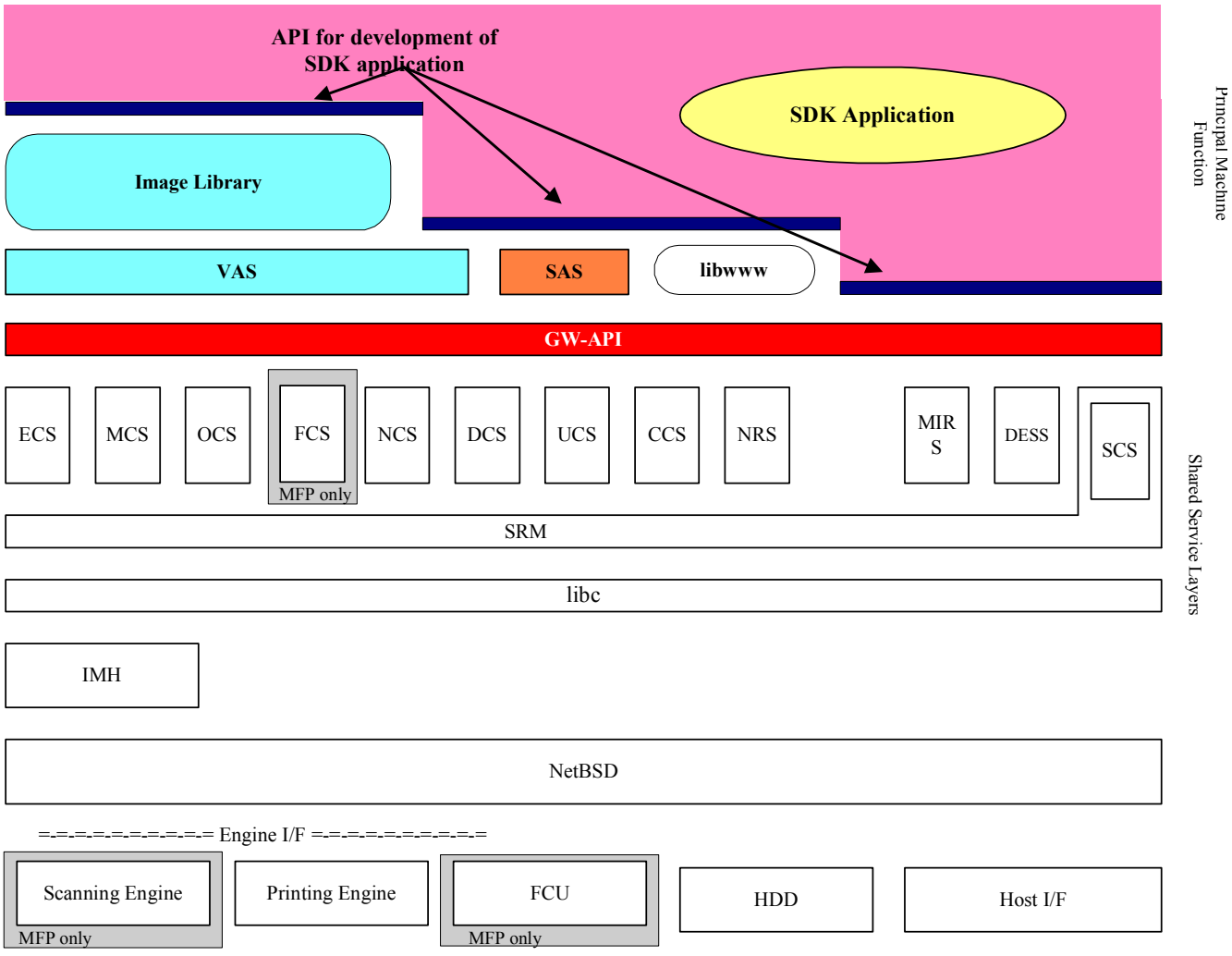


Fig. 3: DSDK – MFP/LP Hardware Configuration

Data Flow

Scanning Functions: Sending Data over the Network with the Copier and Scanner (MFP models only)

- DSDK applications are capable of utilizing the scanning features of the MFP Copier and Scanner. For an overview of the MFP Copier and Scanner operations, please refer to Copier (MFP Models Only) and Scanner (MFP Models Only).

- The Image Library calls the ECS, MCS (IMH) and SCS service layers via the VAS and GW-API, after which Scanner or Copier operations are initiated (e.g. Scanning→ HDD storage→ Loading from memory→ Printing). The Image Library is a static library, and is contained within the SD card along with the SD application(s). The application generates and controls its user interface by calling the operation panel control I/F (OCS).

- When sending a scanned image stored in the machine over the network to a network-connected server or client station, the raw file is read out of HDD memory and then converted from Ricoh-original format to Unix FFS (Fast File System) format. The image data is converted to TIFF, JPEG or PDF format, after which the SDK application transmits the entire file over the network using the NCS (Type 1) or by opening its own unique socket (Types 1 and 2).

FAX Functions (MFP models only)

- Of the several FAX transmission features provided by the FCS (Fax Control Service), SDK applications are allowed to utilize the LAN FAX feature only. Therefore, as the MFP only allows LAN FAX to send to one destination at a time, the SDK application is not able to utilize such features as Broadcasting or Batch Transmission.

- With FAX reception, SDK applications are able to access FAX images that have been received and stored in the MFP HDD, and then transfer them to DeskTopBinder or Desk Top Editor for Production.
  Note: Incoming FAX images are automatically stored to the HDD when “Store Incoming Faxes” is enabled.

- When the FCU (Fax Control Unit) receives an incoming FAX, a notification is sent to the FCS, which then writes the incoming data to the work area of the HDD. The FCS informs libFAX that a transmission has been received, after which libFAX is able to access the file and retrieve it from the HDD. If the file is to be transferred to DeskTopBinder or Desk Top Editor For Production, it is converted to TIFF format and then sent to its destination.

Network Functions

- As mentioned above, a Type 1 SDK application is able to perform network communication either by using the NCS or by opening and closing its own unique socket. Since Type 2 applications are Java-based, they must use the network classes provided by Sun Microsystems, and are therefore restricted to socket-based network communication.

Printer Functions

- SDK applications are able to make use of a printer data filter, which allows the application to edit the incoming printing data received by the MFP/LP, convert it to a different PDL, and change job control commands such as the paper tray selection or printing mode. Following this, the SDK application sends the edited PDL data to the printer port of the loop-back address (the 127.0.0.1 local address), which the MFP/LP Printer function then receives just as if the PDL data had come directly from an external source. The data then follows the normal flow described in section 2.2 and is printed out by the printing engine.

Machine Administrative Functions (MFP models only)

- In addition to the principal machine functions of the MFP/LP (e.g. Printer, GWWS), once installed, the SDK application can be selected in the “Function Priority Setting” so that it its screen is displayed when the main power is turned ON and the MFP/LP reaches the Ready condition.

- It is possible to create a user interface for communication with a network-connected authentication server in order to authenticate individual machine users, thereby restricting the use of the application. The user interface can be customized for each individual user, and will automatically log out the user and return to the default screen if no operations have been performed after a certain amount of time has passed.

- It is also possible to maintain a machine usage log. The SDK application creates the log files and writes them to the SDK area of the HDD.

24. Data Security Considerations

Preventing the Installation of Illegal Applications

- The following are used to prevent the installation of illegal SDK applications or altering of authorized SDK applications already installed in the MFP/LP:
  - Product ID (comprised of a vendor code, country code and code representing the application type)
  - SDK Authentication (Types 1 and 2)
  - Digital Authentication (Type 2)

- When the Vendor begins developing an SDK application for installation on the MFP/LP, a contract is created between the Vendor and Ricoh. In addition to the necessity for strict confidentiality of information, this contract also specifies the scope of responsibilities regarding product quality, as well as all the details of sales-related agreements made between both sides.

- Having agreed to the terms of the contract, the Vendor requests Ricoh to assign and provide a product ID for the proposed application. In addition to being a completely unique number by which the Vendor can be identified should the need arise, the product ID is also used by the Vendor to create an installation directory for the SDK application and by Ricoh to authenticate the application through SDK Authentication. As explained below, without the correct product ID, there is no way to install the SDK application on the MFP/LP.

- The MFP/LP is designed so that each SDK application, once authenticated, is installed in its own unique directory. This ensures that the objects, data files and other contents of one SDK application can never be overwritten or accessed by another.

Authentication of SDK Applications at Installation

The following two processes are performed in order to authenticate SDK applications, which ensures that only authorized applications can be installed in the MFP/LP, as well as to control the range of operations and access of the applications once installed.

SDK Authentication (Types 1 and 2)

- Once the development of the SDK application has been completed, and Ricoh has authorized its installation on the MFP/LP model(s) in question, Ricoh provides the Vendor with: 1) a file containing the unique product ID mentioned above in its raw form, and 2) a "key file," which contains two hash values generated from the product ID and SDK application object code, which are then embedded inside randomly-generated data. The locations of these hash values inside the key file are not disclosed to the Vendor.

- Using a special tool, Ricoh generates a unique key file for every SDK application that is approved. Among the entire group of specialists at Ricoh engaged in SDK application-related activities, only a select number of engineers have been granted the access rights to use and manage this special tool.

- When the SD card is inserted in the MFP/LP slot, the SAS reads the raw form of the product ID contained in the product ID file, as well as the hash value for the ID contained in the key file. The SAS then applies a unique hash function to the raw form of the product ID, and compares the resulting value with the hash value read from the key file.

- If these two values match, the SAS then reads the raw form of the SDK application object code stored in the SD card, as well as the hash value for the code contained in the key file. The SAS applies a unique hash function to the entire code, and then compares the resulting value with the hash value read from the keyfile. If these two values match, the name of the SDK application appears on the installation screen and the application can be installed on the MFP/LP.

- As demonstrated above, it is not possible to install an SDK application on the MFP/LP unless both of the following conditions have been satisfied:
  - The SD card contains the key file and raw form of the product ID provided by Ricoh, as well as the raw form of the application object code developed by the Vendor, AND
  - The two hash values generated by the MFP/LP for the product ID and application object code match those contained in the key file on the SD card.

Digital Authentication (Type 2 only)

- For Type 2 applications, Ricoh embeds a digital signature inside the JAR files received from the Vendor, assigns an appropriate access level, and then returns the files to the Vendor. This allows the MFP/LP to authenticate the application as well as restrict its operations once installed.

- As a general rule, Ricoh assigns relatively restricted access privileges to Type 2 applications. These applications are normally prohibited from performing operations such as file storage to MFP/LP media or opening and closing sockets to communicate over the network. Vendors who wish to utilize such functions must make this request to Ricoh when applying for the digital signature. After having fully ascertained all relevant details on the proposed SDK application, including the Vendor's specific purpose for using the application on the MFP/LP in question, and having determined that the application poses no security threat to the MFP/LP, Ricoh approves the application and assigns the appropriate access level.

Prevention of Access to Address Book Data and Machine Management Data

- Regardless of the access level granted by Ricoh, SDK applications are not able to access Address Book data, internal log data or machine settings stored in the NV-RAM. It is therefore not possible for the SDK application to perform any operations whatsoever on this data, such as making unauthorized copies of the data, transmitting it over the network or saving it to an SD card or other media.

Protection Against Attacks on Principal MFP/LP Functions, Prevention of Damage to the System

Buffer Overflow Attacks on the MFP/LP VM

- After completing the development of the SDK application, the Vendor must apply to Ricoh for the items necessary to carry out the SDK Authentication and/or Digital Authentication processes described above, and at that time declare the expected VM consumption of the application. The proper method for measuring VM is described in the SDK Development Kit provided by Ricoh to the Vendor. Ricoh then performs tests on the proposed application to verify that the actual VM consumption matches that which the Vendor has stated on the application form, and then makes a judgment as to whether or not to approve the application and provide the Vendor with the requested authentication items.

Alteration or Deletion of MFP/LP Principal Function Program Objects

- As mentioned above in section 3.1, each SDK application is installed in its own unique directory on the HDD, which is determined by its unique product ID. It is impossible for the application to access any other areas.

- Even in the event that an SDK application attempted to write a large amount of data to the SD card or MFP/LP HDD, e.g. with the aim of rendering machine principal functions unable to write data, this would not succeed since the application cannot access any area aside of its own isolated partition on the HDD. In addition, as a general rule, Ricoh prohibits SDK applications from writing to any machine media or SD cards. Even in cases where Ricoh has given the application writing capabilities upon request from the Vendor, the application is only able to write to a specialized SD card for SDK applications.

Protection Against Attacks from External Sources

- As mentioned in section 2.3, an SDK application is able to perform network communication either by using the NCS (Type 1) or by opening and closing its own unique socket (Types 1 and 2). In the latter case, all communication including the content of all messages and data exchanged is encrypted, and specialized protocols and authentication procedures are employed. As a result, these safeguards protect the MFP/LP from any attacks from external sources.

Certification of the SDK Application

- Having completed the development of the production-level (product release) version of the SDK application, the Vendor must then request Ricoh to certify the application. When applying for Ricoh certification, the Vendor must provide Ricoh with the application's functional specifications, entire object code and all relevant evaluation results.

- Following this, Ricoh examines the information provided by the Vendor to ascertain in detail the full scope of the operations of the application, as well as to what extent the application has already been tested. These results are then documented (If deemed necessary, Ricoh may perform further testing on the application). If Ricoh determines that the application poses no particular issues or problems, the Vendor is provided with the necessary authentication files. By providing these files, Ricoh is certifying the application.

- If the Vendor then makes any changes to the application after receiving the authentication files from Ricoh, this Vendor must go through the entire certification process again to obtain new authentication files. It is therefore impossible for an SDK application to be successfully installed on the MFP/LP without the correct authentication files.

- Ricoh utilizes this system to manage and control the specifications, operations and quality of SDK applications developed by Vendors, preventing the illegal installation of any SDK application that has not been fully certified as described above.